U.S. Department of Homeland Security

United States Coast Guard

POLICY ADVISORY COUNCIL (PAC) DOCUMENT REGISTRY

FEBRUARY 2018

REGISTRY OF POLICY ADVISORY COUNCIL (PAC) DECISIONS

YEAR	PAC # / Description	Change	Status	Notes
2003				
01-03-	Facilities with Foreign Mega Yachts	3	Rescinded	
02-03-	Foreign Vessels Less than 500 Gross Tons		Rescinded	
03-03-	Remote Facilities	3	Rescinded	**Incorporated in 33 CFR Part 105**
04-03-	Passenger Vessels and Terminals		Rescinded	
05-03-	Variable (Intermittent) Risk Operations (Facilities)	1	Active	
06-03-	Screening Procedures		Rescinded	
07-03-	ASP's for SOLAS Vessels		Active	
2004				
09-04-	Inland Containers		Rescinded	
10-04-	Bulk Cargo Facilities	4	Active	
11-04-	Seasonal Operating Facilities		Rescinded	
13-04-	Facilities Fueling Vessels & Facilities Handling Wastewaters	3	Active	
14-04-	Security of Marine Events of National Significance	1	Rescinded	**Replaced by CG-FAC Policy Letter 01-16**
15-04-	Marking and Monitoring Security Zones		Rescinded	
16-04-	Drilling Mud & Other Oil Field Wastes	6	Active	
17-04-	Inbound Cargo and Passengers		Rescinded	
18-04-	Domestic Vessels Traveling to British Virgin Islands		Rescinded	
19-04-	Non-SOLAS Vessels Traveling Between the US and Canada	1	Rescinded	
20-04-	Certain Dangerous Cargo Facilities		On Hold	
21-04-	Slops, Heels and Other Residuals		Active	
22-04-	Declarations of Security		Rescinded	
23-04-	Drilling Brine (Zinc Bromide)	2	Active	
24-04-	Public Access Facilities	1	Active	**Also See NVIC 09-02 Change 4**
25-04-	Interim International Ship Security Certificates (ISSC)	1	Rescinded	
26-04-	MTSA and ISPS Tonnage Applicability		Active	
27-04-	Facilities Receiving U.S. Vessel on Domestic Voyages		Rescinded	
28-04-	Foreign Barges		Active	
29-04-	Security of Empty Cargo Containers		Rescinded	
30-04-	Credentialing of Federal, State and Local Officials		Rescinded	
31-04-	Lightering Operations		Active	
32-04-	Coupled T-Boats		Rescinded	
33-04-	Caustic Soda Solution	2	Active	
34-04-	Locking of Public Access Facilities	1	Active	
35-04-	Cruise Ships, Tenders and Public Access Facilities	2	Active	
36-04-	VSP Amendments		Rescinded	
37-04-	Screening Guidance to Private Security Firms and Consultants		Rescinded	
38-04-	Excursion Vessels		Rescinded	
39-04-	Communications Between Ships Security Officers and Company Security Officers		Rescinded	
40-04-	Determining Which Vessels are Subject to SOLAS		Rescinded	
41-04-	Shipyard Security	1	Active	
42-04-	Security of Crew and Passenger Identification		Rescinded	
43-04-	Facilities Receiving Vessels from Canada		On Hold	
44-04-	Determining Which Foreign Yachts Are Subject To SOLAS		Active	
45-04-	Timelines for MTSA Required Exercises	2	Active	
48-04-	Capability to Continuously Monitor		Active	

YEAR	PAC # / Description	Change	Status	Notes
2005				
49-05-	Personal Identification		Rescinded	
50-05-	Facilities Located in the Gulf of Mexico		Rescinded	
51-05-	Urea Ammonium Nitrate Solution (2% or less NH3)		Active	
52-05-	Personnel Conducting Security Audits	1	Rescinded	**Information available in 33 CFR subchapter H**
53-05-	Towing Vessels Moving Regulated Barges NOT Carrying CDCs		Active	
55-05-	Auditing of Alternative Security Programs	1	Rescinded	
56-05-	Companies Withdrawing from Alternate Security Plans		Rescinded	
57-05-	Exceptions to Part 105 Applicability for Oil and Natural Gas Facilities		Active	
59-05-	Facilities and Vessels Receiving Exercise Credit for Participating in Area Maritime Security Plan Exercises		Active	
60-05-	US Flagged Small Passenger Vessels with SOLAS Documents		Active	
61-05-	Implementation of AWO's Amended ASP		Rescinded	
2007				
01-07-	TWIC and Law Enforcement Officials and Other Regulatory Agencies		Active	
02-07-	Escorting Aboard US Flagged Vessels Operating in Foreign Waters		Active	
2008				
01-08-	Redefining Secure Areas and Acceptable Access Control		Active	
02-08-	Federal & Law Enforcement Officials Authority to Act as Escorts on Regulated Facilities and Vessels		Active	
03-08-	Escorting Standards for Persons in Addition to Crew		Active	
04-08-	TWIC Applicability Regarding Railroad Police Officers		Rescinded	
05-08-	TWIC Requirements and Rail Access Into Secure Areas		Active	
07-08-	TWIC Activation & Fingerprint Reject Impacts - Limited Equivalent Security Measure	8	Rescinded	**Replaced by CG-FAC Policy Letter 12-05**
08-08-	Private, Non-Governmental Emergency Responders Access to Regulated Facilities and Vessels for Mutual Aid Response		Rescinded	
09-08-	Bulk Grain, Oil Seed, and Edible Oils Facilities and Redefinition of Secure Areas		On Hold	
2009				
01-09-	U.S. Flag Overnight Passenger Vessels in Domestic Trade "Other Persons in Crew"		Active	
02-09-	Training Requirements for Escort on Regulated Facilities and Vessels		Active	
03-09-	TWIC 30 Day Unescorted Access Extension to Individuals Awaiting Receipt of a Replacement TWIC	4	Rescinded	**Replaced by CG-FAC Policy Letter 12-04**
05-09-	Limited Equivalent Security Measures for MTSA Regulated Vessels, CG Credentialed and OCS Facilities		Rescinded	**Replaced by CG-FAC Policy Letter 12-04**
06-09-	Escorting Requirements for Passengers Traveling with Commercial Truck Drivers		Active	
07-09-	Foreign Flagged Cruise Ship Crew & Escorting through Secure and Restricted Areas		On Hold	
08-09-	Incorporating TWIC into Existing Physical Access Control Systems	1	Active	
09-09-	Waiving Facilities that Transfer and Store Asphalt	1	Active	
10-09-	Defining what areas of a Barge Fleeting Facility are subject to Subchapter H Part 105 Security Requirements		Active	
2011				
01-11-	Voluntary Use of TWIC Readers		Active	
02-11-	Waiving Facilities that Transfer Certain Low Risk Commodities		Rescinded	

MTSA/ISPS POLICY ADVISORY COUNCIL

April 22, 2004

Issue/Discussion/Decision

Variable (Intermittent) Risk Operations (Facilities)

05-03 Change 1

***CG-FAC Edited 2018**

FINAL

Issue: How will 33 CFR part 105 be implemented for facilities that perform regulated functions on an intermittent basis?

Discussion: Currently, 33 CFR 105 does not facilitate turning a Facility Security Plan (FSP) off and on. However, the Coast Guard recognizes that every facility is not at risk for a transportation security incident (TSI) at all times. An example of a variable risk operation could be a facility that is regulated only because they receive a foreign flagged vessel several times a year. Questions have been raised regarding whether a facility needs to implement its security plan when the threat of a TSI is low.

Decision: Many facilities perform MTSA regulated functions intermittently and may implement variable security measures based on the level of risk while not actively receiving MTSA-regulated or foreign flagged vessels or storing hazardous cargo intended for MTSA-regulated vessels. Based on a thorough, risk-based facility security assessment, the FSP must address security measures to be implemented when regulated activities cause the level of risk to increase. When the threat of a TSI is low the facility may reduce its security posture, but may not totally suspend its FSP. The security plan must also include measures to be used prior to resuming full MTSA-regulated operations, such as sweeping the facility after re-establishing full perimeter control.

MTSA/ISPS POLICY ADVISORY COUNCIL

May 13, 2004

Issue/Discussion/Decision

ASP's for SOLAS Vessels

07-03

*CG-FAC Edited 2018

FINAL

Issue: Is the use of an Alternative Security Program (ASP) permitted for vessels subject to ISPS or SOLAS?

Discussion: A number of vessels that belong to The American Waterways Operators (AWO), the Passenger Vessel Association (PVA) and the Offshore Marine Service Association (OMSA) sail on international voyages. Questions have been raised whether those vessels can subscribe to an ASP, since 33 CFR 104.140(b) indicates that a vessel that is subject to SOLAS may not use such an alternative.

Decision: Vessels subject to SOLAS subscribing to an ASP must submit an International Vessel Security Plan which satisfies the requirements of ISPS to the Marine Safety Center (MSC) for review and approval. Generally, the vessel has the following two options:

Scenario One: An ASP sponsoring organization such as OMSA may choose to submit a Vessel Security Plan to the MSC for review and approval. Once this plan is approved, the sponsor organization may provide this plan to its members. The members may then use this approved plan as a template for developing their own plans; individualizing pages that list the vessel particulars, such as the Vessel Security Officer, official number, etc. Each vessel would then submit their own plan to the MSC for review and approval. The sponsor organization will provide additional details to their members on what must be submitted to the MSC.

Scenario Two: An ASP sponsoring organization such as AWO may choose to submit an international addendum to the MSC for review and approval. An international addendum will include certain requirements of ISPS that are not addressed in the ASP and any specific sections of the ASP that must be developed by the vessel operator, such as a vessel-specific security assessment report and an on-scene survey. This approved addendum will be added to vessel-specific material and submitted to the Marine Safety Center by a vessel operator and be considered a Vessel Security Plan. Vessel operators should contact their sponsoring organization to find out exactly what must be submitted to the MSC to be considered a complete VSP submission. Upon MSC approval of the VSP the vessel is eligible to receive an International Ship Security Certificate (ISSC). Subscribers to an ASP should contact their sponsoring organization to determine if an international addendum has been submitted and/or approved before providing anything to the Marine Safety Center.

Vessels must be in full compliance and maintain the security measures outlined in the approved VSP. For uninspected vessels, the VSP may include variables that will NOT be enacted when a vessel is operating only on domestic voyages, or state that the plan may be "turned off" during certain voyages. (This may be considered as downgrading). These variables must be clearly stated in the approved VSP. Furthermore, when variable security measures are enacted, the plan must also state the process that a vessel must undergo before returning to MTSA/ISPS operations. (This is considered as upgrading). For example, a tug operating on a voyage subject to MTSA/ISPS is required to do a DoS at MARSEC 2 and 3. The plan may state that when operating on non- regulated voyages, the tug may downgrade its security stance, eliminate the access control portion of their plan, and not complete a DoS. When the vessel returns to MTSA/ISPS operations, the vessel must follow its plan for re-establishing security measures through processes such as conducting a full sweep/search of the vessel to ensure a secure access control program.

MTSA/ISPS POLICY ADVISORY COUNCIL

March 25, 2004

Issue/Discussion/Decision

Bulk Cargo Facilities

10-04 Change 4

*CG-FAC Edited 2018

FINAL

Issue: 33 CFR 105.105(a)(1) states that any facility regulated under 33 CFR part 126 will have to comply with the requirements of 33 CFR part 105 in its entirety. However, the applicability of 33 CFR part 126 includes "Materials Hazardous only in Bulk" which are regulated under 46 CFR part 148. Was it the intent of the MTSA regulations to include all of the cargos listed in 46 CFR part 148, or are there some cargoes in that list that were not meant to be subject to the requirements of the regulations?

Discussion: There are three aspects of this issue that must be discussed: the cargo, the means of delivery and the facility that receives the means of delivery.

Cargo: Materials Hazardous only in Bulk (MHB's) are regulated domestically by 46 CFR part 148 and internationally by the IMO Code of Safe Practice for Solid Bulk Cargoes (BC Code). However, there are some cargoes in 46 CFR part 148 or the BC Code that pose little to no risk from a security perspective. Those cargos are listed in Annex I to this decision. For that reason, vessels carrying cargo regulated pursuant 46 CFR Subchapter N (except those considered a certain dangerous cargo) may send a request to Commandant (CG-FAC-2) requesting to be considered for a waiver from the requirements of 33 CFR part 104 in accordance with 33 CFR part 104.130.

Means of Delivery: 33 CFR 104 identifies a number of categories of vessels that are considered at risk for security purposes. Vessels carrying a cargo identified in Annex I are not subject to the requirements of 33 CFR part 104 unless one of the other applicability factors of 33 CFR 104.105 applies.

Facility: Generally, it is the intent of the regulations that facilities that receive vessels that are required to comply with 33 CFR 104 for any reason are required to comply with 33 CFR 105. For example, the facility that receives the self-propelled vessel carrying an Annex I cargo that is greater than 100 gross register tons and inspected pursuant to 46 CFR Subchapter I must comply with 33 CFR 105.

A facility that receives a barge that does not engage on international voyages or is not subject to inspection that only carries Annex I cargoes or other non-regulated may send a request to Commandant (CG-FAC-2) to be considered for a waiver from the requirements of 33 CFR part 105 in accordance with 33 CFR part 104.130.

Decision: We have conducted an assessment of the cargoes listed in Annex I and have determined that they pose a lower risk of causing transportation security incident. Since a vessel that handles these cargoes is not subject to 33 CFR part 104, unless another applicability factor is involved, the Coast Guard will consider waiving facilities that only receives Annex I cargoes from a vessel not otherwise subject to 33 CFR part 104. Those facilities wishing to be considered for a waiver may send a request to Commandant (CG-FAC-2).

****

Annex I

IMO Code of Safe Practice for Solid Bulk Cargoes (BC Code):

- Brown Coal Briquettes (Lignite)
- Calcined Pyrites (Pyritic ash, Fly ash)
- Charcoal
- Coal
- Direct Reduced Iron (Hot & Cold molded)
- Ferrosilicon, containing 25% to 30% silicon or 90% or more silicon (including briquettes) *****
- Fluorspar (Calcium Fluoride)
- Magnesia (unslaked)
- Metal Sulphide Concentrates
- Peat Moss
- Pitch Prill (Prilled Coal Tar, Pencil Pitch)
- Silicomanganese (with a silicon content of 25% or more)
- Vanadium Ore
- Woodchips
- Wood Pulp Pellets

46 CFR part 148:

- Ferrophosphorus
- Lime, unslaked
- Petroleum coke, calcined
- Petroleum coke, uncalcined
- Sawdust

MTSA/ISPS POLICY ADVISORY COUNCIL

August 3, 2017

Issue/Discussion/Decision

Facilities Fueling Vessels & Facilities Handling Wastewaters
13-04 Change 3

*CG-FAC Edited 2018

Issue: How will 33 CFR part 105 be implemented at facilities that store small amounts of oil products and are applicable to MTSA only because they are regulated by 33 CFR part 154?

Discussion: Numerous fueling docks receive vessels capable of receiving more than 250 barrels of oil. These vessels are primarily fishing, recreational, or small passenger vessels.

There are also facilities that transfer oily wastewaters, industrial wastewaters, and wash water from barges. These facilities may be designated as shipyards, barge cleaning & repair services, water reclamation & recycling facilities, and oily & industrial wastewater disposal facilities. In most cases the oil content of the wastewater is very small.

Additionally, some shipyards may transfer small amounts of fuel from vessels under repair into storage tanks to be transferred back to the vessel when repairs are completed.

Could these facilities be considered for a waiver?

Decision: Facilities wishing to have their operations examined in consideration for a waiver may forward a request to Commandant (CG-FAC-2) in accordance with 33 CFR 105.130. The request letter should address the following areas:

1. Does the facility store more than 42,000 aggregate gallons of all oils regulated by 33 CFR part 154;
2. Does the facility store any other regulated cargo;
3. Does the facility receive vessels subject to SOLAS;
4. Does the facility receive foreign flagged vessels; and,
5. Is the facility regulated under any other applicability factor?

Other Considerations: Are operational procedures or products handled by the facility considered to be a high risk factor for causing or contributing to a transportation security incident?

MTSA/ISPS POLICY ADVISORY COUNCIL

DEC 6, 2005

Issue/Discussion/Decision

Drilling Mud & Other Oil Field Wastes
16-04 Change 6

*CG-FAC Edited 2018

FINAL

Issue: Drilling mud describes a wide variety of compounds used to lubricate and cool oil and gas drilling bits as well as flush ground up solids to the surface. The compounds are injected in the drill pipe and partially recovered (some remains in the well) and disposed of along with much of the cuttings that are flushed to the surface of the well. Should vessels certificated under 46 CFR Subchapter D or facilities regulated under 33 CFR part 154 that transport or handle oil field wastes be waived from the requirements in 33 CFR parts 104 and 105?

Discussion: Drilling mud (low toxicity) is listed in 46 Subchapter D, Table 30.25-1. It is considered to be a Grade E cargo and is required to be carried in barges certificated under 46 CFR Subchapter D. Under these circumstances, vessels carrying this cargo would be required to implement security plans. However, upon consultation with Coast Guard Office of Environmental Response Policy (CG-MER) and Coast Guard Office of Design and Engineering Standards (CG-ENG), we have determined that drilling mud and other oil field wastes pose a low risk of causing a transportation security incident if these materials were used maliciously.

Decision: We have conducted an assessment of drilling mud and other oil field wastes as described in NVIC 07-87 (Guidance on Waterborne Transport of Oil Field Wastes), and have determined that this cargo poses a lower risk of causing a transportation security incident. NVIC 07-87 also notes that oil field wastes may have additional hazards other than oil and it is the responsibility of the shipper to comply with all relevant regulations for all components of the wastes. As a result, the Coast Guard may waive vessels that handle oil field wastes from 33 CFR part 104 unless another applicability factor is involved. Likewise, the Coast Guard may waive facilities that receive these materials from vessels not otherwise subject to 33 CFR part 104 unless another applicability factor is involved. These waived vessels and facilities remain subject to parts 101 and 103 of 33 CFR Subchapter H.

Vessel Examples: Barges that alternate between carrying oil field wastes and other cargoes listed in 46 CFR Table 30.25-1, "List of Flammable and Combustible Bulk Liquids Cargoes", would be required to comply with 33 CFR part 104. Barges that do not engage on international voyages that carry only oil field wastes or other non-regulated cargoes are not required to comply with 33 CFR part 104. All other vessels listed in 33 CFR 104.105, applicability, are subject to 33 CFR 104.

Facility Examples: Facilities that receive barges that do not engage on international voyages that carry drilling mud and other oil field wastes may apply for a waiver from the requirements of 33 CFR part 105, unless other applicability factors exist. As part of a waiver request the owner/operator must identify and determine the hazard class of all oil field wastes handled. All other facilities listed in 33 CFR 105.105, applicability, are subject to 33 CFR 105.

Vessels or facilities wishing to have their operations examined in consideration for a waiver may send a request to Commandant (CG-FAC-2) in accordance with 33 CFR 104.130 or 105.130.

MTSA/ISPS POLICY ADVISORY COUNCIL

May 6, 2004

Issue/Discussion/Decision

Slops, Heels, and Other Residuals

21-04

*CG-FAC Edited 2018

FINAL

Issue: Are vessels carrying slops and residuals required to comply with MTSA?

Discussion: Many vessels and barges travel throughout different Captain of the Port zones with small amounts of residual Certain Dangerous Cargoes (CDC) onboard. Sometimes these vessels receive Tank Dry Certificates, indicating that the vessel no longer carries cargo. These Tank Dry Certificates are issued, even though the tank may not be gas freed. For the shipment of hazardous materials regulated under 49 CFR Subchapter C, "an empty packaging containing only the residue of a hazardous material shall be offered for transportation and transported in the same manner as when it previously contained a greater quantity of that hazardous material". See 49 CFR 173.29. The MTSA regulations and 33 CFR Subpart C, entitled Notification of Arrival, Hazardous Conditions, and Certain Dangerous Cargoes, do not specifically address situations with empty holds or tanks.

Many regulations are dependent on whether there are cargoes onboard, most notably including those regulations requiring Declarations of Security (33 CFR 105.245) and additional requirements for CDC Facilities (33 CFR 105.295). Will these regulations be implemented when vessels with CDC residuals or slops are moored alongside facilities?

Decision: A certificated vessel must implement its Vessel Security Plan (VSP) at all times. Similar to the passenger vessel that is certificated for 150 passengers but carries less than this number; a cargo vessel carrying small amounts of regulated cargo would be required to implement its entire VSP. When this vessel has a Gas Free Certificate, variable security measures may be adopted for the periods of time when the vessel is out of service and not carrying regulated cargoes. In this instance, the VSP must address the variable measures that the vessel will use as well as those measures that it will use before resuming operations.

MTSA/ISPS POLICY ADVISORY COUNCIL

June 30, 2004

Issue/Discussion/Decision

Drilling Brine (Zinc Bromide)
23-04 Change 2

*CG-FAC Edited 2018

FINAL

Issue: Should vessels and facilities handling drilling brine (zinc bromide) be waived from the requirements in 33 CFR Parts 104 and 105.

Discussion: Drilling brine, or zinc bromide, is listed in 46 CFR Subchapter O, Table 2 to part 153. It is considered to be a Category B Noxious Liquid Substance by MARPOL 73/78 and oceangoing ships carrying this cargo in bulk would be required to be certificated under 33 CFR Subchapter O. Under these circumstances, vessels carrying this cargo would be required to implement security plans and the facilities that receive these vessels would also have to implement security plans. However, upon consultation with the Coast Guard Office of Design and Engineering Standards (CG-ENG), we have determined that drilling brine poses a low risk of causing or being involved in a transportation security incident even if this cargo was used maliciously.

Decision: The Coast Guard may waive barges that handle drilling brine as not being subject to 33 CFR part 104 unless another applicability factor is involved. Likewise, the Coast Guard may waive facilities that receive drilling brine from barges not otherwise subject to 33 CFR part 104 unless another applicability factor is involved. These waived barges and facilities remain subject to sections 101 and 103 of 33 CFR Subchapter H.

Barge Examples: A barge that alternates between carrying drilling brine and other regulated cargoes would be required to comply with 33 CFR part 104. Also, a self-propelled vessel carrying drilling brine that is greater than 100 gross register tons and inspected pursuant to 46 CFR Subchapter I or Subchapter L must comply with 33 CFR part 104. A barge that does not engage on international voyages that only carries drilling brine or other non-regulated cargoes may send a request to have their operations examined in consideration for a waiver to Commandant (CG-FAC-2) in accordance with 33 CFR 104.130.

Facility Examples: A facility that receives any self-propelled vessel carrying drilling brine must comply with 33 CFR part 105. A facility that receives a barge that does not engage on international voyages that carries only drilling brine may send a request to have their operations examined in consideration for a waiver to Commandant (CG-FAC-2) in accordance with 33 CFR 105.130.

MTSA/ISPS POLICY ADVISORY COUNCIL

March 25, 2005

Issue/Discussion/Decision

Public Access Facilities

24-04 Change 1

*CG-FAC Edited 2018

FINAL

Issue: The purpose of the guidance in these enclosures is to provide instruction for COTPs and facility owners or operators regarding application, review, and granting of Public Access Facility (PAF) designations per 33 CFR 105.110(d). Designation of a PAF does not constitute total exemption of 33 CFR part 105. To ensure national consistency, COTPs shall incorporate this guidance when considering a PAF designation request.

DEFINITION OF PUBLIC ACCESS FACILITY

1. In order to be considered a Public Access Facility, the facility must fall under the requirements of 33 CFR 105.105(a)(2): "Facility that receives vessels certificated to carry more than 150 passengers."

A facility that falls under any other paragraph of the 105 applicability would not be able to meet the definition of a Public Access Facility because those facilities would handle cargo. According to the comments section of the Federal Register, "We have not allowed public access facilities to be designated if they receive vessels such as cargo vessels because such cargo-handling operations require additional security measures."

2. In order to be considered a Public Access Facility, the facility must meet the definition outlined in part 101.105.

Under the Public Access Facility definition, there are 3 paragraphs. A facility must meet all 3 paragraphs to meet the definition.

- *Facility is used primarily for recreation, entertainment, retail or tourism*
- *Has minimal infrastructure*
- *Receive no 104-regulated vessels except passenger vessels*
  - *No passenger vessels certificated to carry vehicles*
  - *No cruise ships*
  - *No passenger vessels subject to SOLAS*

3. The 33 CFR 101.105 definition of Public Access Facility, paragraph (1) talks about a facility being used "primarily for purposes such as recreation, entertainment, retail or tourism."

Does this apply to a commuter ferry dock or landing, which receives vessels that carry passengers and may also be used for recreation purposes, such as people fishing off the dock? Yes, if the public has access to the dock, they may use the dock at any time for recreation therefore the ferry does not have exclusive use of the dock. The dock is multi-use, has public access, minimal infrastructure and there does not seem to be a need to apply all of 105 to this dock. The sentence says "such as", so the four purposes listed are examples, and are not all-inclusive.

4. The 33 CFR 101.105 definition of Public Access Facility, paragraph (1) says that the dock may <u>not</u> be primarily used for receiving vessels subject to part 104.

A dock that exists solely for the purpose of receiving a 104 vessel cannot be considered a Public Access Facility. An example of this is as follows: A hotel has a dock that receives a 104 vessel. The dock has minimal infrastructure, but the public does not have access to the dock. The hotel restricts access to the dock to only those going aboard the vessel for a tour. Since the dock is only there because it is used to receive the 104 vessel, it falls under the requirement of 105, and cannot be considered a Public Access Facility.

5. If a Public Access Facility shares a boundary with a mall, hotel, stadium or other such structure (that falls under the definition of facility in 101.105) the facility should coordinate security with that entity.

To minimize potential security gaps, for protection of the 104 vessel calling on the PAF, the facility should maintain an open dialogue with the adjoining structure. For example, the PAF may need to know what security measures are in place at the stadium.

6. The boundaries of where to apply PAF security measures will be defined on a case by case basis in conjunction with the COTP.

If a city riverfront dock is two miles long and the 104 vessel only ties up to 100 feet of the riverfront, you may not necessarily need to apply security to the entire two miles. The COTP has the discretion to delineate the boundaries.

7. Some marinas could be considered a PAF.

If the marina dock receives a 104 vessel and is not subject to 33 CFR 154 then it could meet the PAF definition. However, if the marina restricts access to their dock, then the dock does not have public access, and would not meet the definition of a PAF but would be required to submit a facility security plan in accordance with 33 CFR part 105 before receiving a vessel subject to part 104.

8. A restaurant with a dock that receives a 104 vessel could be a PAF.

9. City docks, city walks, river walks, inner harbors and other downtown waterfront areas typically meet the definition of PAF.

10. A facility, which receives only small passenger vessels and does not receive 104 vessels is not a 105 facility and therefore is not considered a PAF.

These faci facilities will fall under the requirements of 101 and 103.

11. A facility that receives cruise ships, car ferries or passenger vessels regulated under SOLAS cannot be designated as PAF's, according to the PAF definition.

These facilities will fall under the requirements of 105.

12. If a location only receives a vessel on a one time basis this location would not be designated as a PAF. An example of this scenario would be a wedding at a backyard pier.

When a vessel goes to a dock only for a one-time event, such as a wedding, the facility should not be required to have a Facility Security Plan. At the same time, it is not feasible to designate the location as public access facility because the dock should not have to maintain these requirements all the time – the vessel is only going to be there once. Plus, if the dock is someone's private dock, and it only has a one-time visit, can the facility reasonably be expected to request a PAF designation? Will they even know about the requirements? The responsibility for security should fall on the regulated vessel. For cases such as these, the vessel should request permission from the COTP to tie up at a non-105 regulated facility by requesting a one-time waiver of the 105 facility regulations.

13. If a vessel makes a stop at a location with no infrastructure - this is not a PAF.

The example for this topic is a 104 vessel which stops at a riverbank and ties up to a tree stump. Another example would be a 104 vessel driving up on the beach. The definition of a facility is "any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction…." At a tree stump or on the beach, there is no structure. Since this is not a facility, it cannot be considered a PAF. The vessel should be held responsible for their security at this location. All of the elements of a DOS must be addressed by the vessel, since there is no "facility" there to cover any of the security measures. Even though a DOS is not required, the vessel shall still document the fact that they arrived at this location. Regulated passenger vessels that engage in this activity must addressed security measures to be implemented in the vessel's VSP. The COTP can spell out what security measures must be implemented at these locations, if needed.

14. A cruise ship arrives in a port and anchors away from the dock. The cruise ship uses their tender to ferry passengers back and forth to the dock, so that passengers may temporarily go ashore and return to the cruise ship. The dock has public access and has minimal infrastructure. Can the location be a Public Access Facility?

No, because the definition of a Public Access Facility says that these locations may not receive passenger vessels subject to SOLAS Chapter XI. The facility must be regulated under 33 CFR 105 and must submit a Facility Security Plan to receive SOLAS vessels. Or, as an alternative, the SOLAS vessel may hire a local ferry ***or T-boat*** *to shuttle passengers back and forth to the shore or* ***PAF*** *rather than use the ship's tender. In this case, the vessel must ensure appropriate security measures are in place to ensure appropriate screening occurs when the passengers return.*

Public Access Facility

The purpose of this guidance is to provide instruction for COTPs and facility owner or operators regarding application, review, and granting Public Access Facility (PAF) designations per 33 CFR 105.110(d). Designation of a PAF does not constitute total exemption of 33 CFR part 105. To ensure national consistency COTPs shall incorporate this guidance when considering PAF designation requests.

Designation of Public Access Facilities (PAF)

PAF Designation Requests

(a) An owner or operator of a facility seeking designation of PAF may make this request to the cognizant COTP. As per 33 CFR 101.105, the definition of a PAF is an area with public access that is primarily used for recreation or entertainment purposes and which primary purpose does not include receiving or servicing only vessels that are regulated under 33 CFR 104. This may include a public pier, wharf, dock, waterside restaurant or marina that contains minimal infrastructure, such as only bollards, cleats, or ticket booths. Tab H provides a sample PAF designation request letter.

Review and Evaluation of Requests

(a) The COTP shall conduct a complete review and evaluation of the PAF designation request. This review and evaluation should also consider the results and impacts related to the AMS Assessment.

(b) To assist the COTP with considering this request, an on-site evaluation may be necessary to verify PAF designation applicability.

Establishment of Conditions

(a) Once PAF designation applicability has been determined, the COTP should coordinate with the owner or operator of the facility to establish conditions for which this designation is granted. Tab G provides required and additional security measures the COTP may impose. To ensure consistency the additional security measures should be limited to those listed in the "Additional Requirements to Review for Applicability" column.

<u>Use of the PAF Security Measures Tool</u>

This tool was developed considering the existing Facility Security regulations. The tool provides required and recommended security measures. The "Required Measures" indicated on the tool, are the minimal security measures applicable to all PAFs.

The "Additional Requirements to Review for Applicability" listed in the tool must be considered and shall be implemented as necessary based on COTP port assessments.

Issuance of Designation Letter

(a) After a complete evaluation of the facility has been conducted and security conditions have been established, the COTP shall issue a PAF Designation Letter. Tab I provides a sample designation letter. At a minimum the designation letter shall include a list of established security conditions that shall be implemented at the PAF. Security conditions shall be included as an enclosure to the designation letter and considered SSI. The PAF owner/operator shall acknowledge and accept these conditions in writing.

(b) A copy of the designation letter and acknowledgement shall be kept on file with the AMS Plan for as long as the designation is valid.

(c) Appropriate MISLE entries, including Facility Identification Number and 24-hour contact number of the individual with security responsibilities shall be completed.

Note: PAFs should be designated in MISLE as a "MTSA Facility – No Plan Required". **[Note for reviewer - Check MISLE for exact entry information].**

Vessel Responsibilities When Calling at a PAF

General Responsibilities

(a) The Vessel Security Plan must address security concerns while at the PAF, per 33 CFR 104.292(d).

(b) The vessel is responsible for implementing all appropriate security measures while at the PAF, however, they may liaison with the PAF to determine who will actually perform security activities.

MARSEC Level Responsibilities

(a) At **MARSEC 1**, the vessel owner/operator, VSO or CSO should contact the Individual with Security Responsibilities at the PAF prior to their first visit to determine security measures that will be in place at the PAF. The appropriate Area Maritime Security Plan includes a list of PAFs, their designated Individuals with Security Responsibilities and COTP requirements.

(b) A vessel that frequently interfaces with the same PAF should also contact the Individual with Security Responsibilities at the PAF when there is a significant change in operations.

(c) If the vessel is unable to contact the PAF prior to arrival, the vessel will perform all security activities and notify the COTP.

MARSEC 2 Responsibilities

(a) At **MARSEC 2**, the vessel owner/operator, VSO or CSO must contact the Individual with Security Responsibilities at the PAF and execute a Declaration of Security (DoS) prior to each visit to determine security measures that will be in place at the PAF.

(b) A vessel that frequently interfaces with the same PAF may execute a continuing DoS for multiple visits with an effective period of not more than 30 days.

(c) If the vessel is unable to contact the PAF prior to arrival, the vessel will perform all security activities and notify the COTP.

MARSEC 3 Responsibilities

(a) At **MARSEC 3**, the vessel owner/operator, VSO or CSO must contact the Individual with Security Responsibilities at the PAF and execute a Declaration of Security (DoS) prior to each visit to determine security measures that will be in place at the PAF.

(b) If the vessel is unable to contact the PAF prior to arrival, the vessel will perform all security activities and notify the COTP.

Compliance and Enforcement

PAF Submissions

(a) Submission of request for Designation as a Public Access Facility.

1) Facilities that were in operation on or before December 31, 2003 should have submitted an FSP and a request for designation as a PAF prior to January 01, 2004.

2) Facilities that have submitted an FSP and wish to be considered for designation as a PAF must submit a request to the cognizant COTP at least 60 days prior to the requested designation date.

   i) Facilities requesting designation as a PAF must comply with the Facility Security Plan submission requirements in 33 CFR 105.410(b) {i.e. 60 days prior to beginning operations} until such time as the PAF designation is granted.

3) If a facility has a change in ownership, the Individual with Security Responsibilities must submit updated contact information to the COTP. The owner/operator of the PAF shall conduct a review of the PAF designation and conditions and notify the COTP of any changes to the facility's operations that may affect security requirements. The new owner/operator or Individual with Security Responsibilities must sign an acknowledgement of the PAF Designation letter and conditions.

(b) After receiving the request, the COTP will either:

1) Approve it with conditions via PAF Designation Letter.

2) Request additional information to make a determination.

3) Disapprove it, with a letter restating requirements under 33 CFR 105 (or stating facility does not meet requirements of 33 CFR 105).

(c) The PAF designation and COTP conditions will be evaluated annually to ensure the designation remains appropriate.

(d) Any changes to the operations or description of the facility must be immediately reported to the COTP.

Enforcement Actions

(Do not include specific enforcement actions in the AMS Plan, include only a general discussion that enforcement actions will be taken when COTP deems necessary.)

(a) Three anticipated types of non-compliance:

(1) Incorrect contact information for Individual with Security Responsibilities

(2) PAF will only be temporarily out of compliance with COTP Conditions

(3) Permanent or frequent non-compliance

(b) Possible enforcement actions:

(1) Informal request for immediate correction/update for administrative discrepancies.

(2) COTP letter request for correction/update within a specified/reasonable timeframe.

(3) COTP Order suspending operations with 104 vessels until in compliance.

(4) Consider civil penalty action.

(5) Revoke their designation as PAF, require full compliance with 33 CFR part 105, and consider issuing a COTP Order with conditions under which they will be allowed to operate until their FSP is approved.

TAB G

PUBLIC ACCESS FACILITY REQUIREMENTS	Required	Additional Requirements to Review for Applicability
Designate, in writing, by name or by title, an Individual with Security Responsibilities and identify how the officer can be contacted at any time	X	
Operate in compliance with the approved PAF requirements.	X	
Report to the COTP within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level	X	
Determine locations where restrictions or prohibitions to prevent unauthorized access to facility and vessel are to be applied for each MARSEC Level.	X	
Document means of enforcement for each identified restriction or prohibition each MARSEC level	X	
Report of all breaches of security, suspicious activities and transportation security incidents IAW AMS plan, Security Incident Procedures and to the National Response Center	X	
Document security incident procedures	X	
Document baseline facility security	X	
An owner or operator whose facility is not in compliance with the requirements of the designation PAF letter must inform the COTP and obtain approval prior to interfacing with a vessel or continuing operations	X	
Maintain ability to have effective communications with MTSA regulated vessels to use facility.	X	
Identify procedures for overnight security to accommodate unattended 104 vessels.		X
Conduct a Facility Security Assessment (FSA) if PAF was identified as location for potential TSI in AMS Assessment.		X
Establish parking procedures and identify designated parking areas, restricting passenger vehicle access to mooring areas.		X
Individual with Security Responsibilities		
Possess knowledge of general vessel and facility operations and conditions	X	
Possess knowledge of vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels	X	
Possess knowledge of emergency response procedures	X	
Possess knowledge of methods of facility security surveys and assessments		X

Possess knowledge of handling sensitive security information and security related communications	X	
Possess knowledge of and must have ability to coordinate security services in accordance with the approved PAF requirements	X	
MARSEC I		
Maintain baseline security	X	

MARSEC II (When 104 regulated vessel at facility)		
Continue MARSEC I requirements	X	
Notify all facility personnel about identified threats and emphasize reporting procedures and stress the need for increased vigilance.	X	
Implement security requirements for restricted areas.	X	
Ensure the execution of Declarations of Security with Masters, Vessel Security Officers or their designated representatives	X	
Increase security personnel from baseline.		X
Limit the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points		X
Limit access to restricted areas by providing physical barriers		X
Ensure adequate security sweeps are conducted to detect dangerous substances or devices.		X
MARSEC III (When 104 regulated vessel at facility)		
Continue MARSEC II requirements	X	
Implement security requirements for restricted areas.	X	
When MTSA regulated vessel is at the facility be prepared to implement additional measures including: (1) the use of waterborne security patrols, (2) use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident, and (3) examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats	X	
Ensure the execution of Declarations of Security with Masters, Vessel Security Officers or their designated representatives	X	X
Suspending access to the facility		X
Evacuating the facility		X
Restricting pedestrian or vehicular movement on the grounds of the facility		X
Increasing security patrols within the facility.		X
Declaration of Security (DOS)		
Each facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a vessel.	X	

The effective period of a continuing DoS at MARSEC Level 1 does not exceed 90 days.		X
The effective period of a continuing DoS at MARSEC Level 2 does not exceed 30 days.		X
When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed.	X	
Maintain a copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period	X	
Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.	X	
The COTP may require, at any time, at any MARSEC Level, any facility subject to this part to implement a DoS with the VSO prior to any vessel-to-facility interface when he or she deems it necessary.		X

Company Letterhead

TAB H

Date

U.S.Coast Guard

Sector/MSU/MSD *(*Name*)*

Attn: Captain of the Port

Address

City, State Zip

Dear Captain of the Port:

We request a PAF designation under the requirements of 33 CFR part 105. We believe our facility meets the definition of "public access facility" under 33 CFR 101.105.[1] [*Describe why your facility meets the definition of a "public access facility": type of facility, primary use of facility, type and frequency of vessels subject to 33 CFR part 104 that use facility*]

For your reference, we have conducted an abbreviated facility security assessment. [*Include results, which could consist of the following:*

Enclose diagram showing access points, both land and water

Enclose map of area showing highways, railroads, etc.

Security measures you and/or vessels will take during facility-vessel interface

Enclose photos of facility and surrounding area]

[1] 33 cfr 101.105 Definitions.

Public access facility means a facility—

(1) That is used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and not for receiving vessels subject to part 104;

(2) That has minimal infrastructure for servicing vessels subject to part 104 of this chapter; and

(3) That receives only:

(i) Vessels not subject to part 104 of this chapter, or

(ii) Passenger vessels, except:

(A) Ferries certificated to carry vehicles;

(B) Cruise ships; or

(C) Passenger vessels subject to SOLAS Chapter XI

We will implement the following security measures at the various MARSEC levels: [*List security measures the facility will follow at MARSEC Levels 1, 2, and 3*].

The following personnel are responsible for implementing security measures: [*Detail primary and alternate points of contact and twenty-four hour contact phone number, fax, and email information*].
I understand that under 33 CFR 105.110, the Captain of the Port (COTP) may establish conditions for the facility designation as a PAF and must ensure adequate security is maintained. I further understand that under 33 CFR 105.110 the COTP may withdraw the designation of public access facility at any time the owner or operator fails to comply with any requirement of the COTP as a condition of the designation or any measure ordered by the COTP [pursuant to existing COTP authority].

Thank you for your consideration. If you have any further questions, you can reach me at [*your contact information*].

Sincerely,

[*J. Smith*]
Security Officer

SENSITIVE SECURITY INFORMATION

U.S. Department of Homeland Security
United States Coast Guard

Captain of the Port
U.S. Coast Guard
Sector/MSU/MSD xxxxxxx
Phone: xxxxxxx
Fax: xxxxxxx

16600
Date

Facility Owner/Operator
Address State

SUBJECT: PUBLIC ACCESS FACILITY DESIGNATION
(COMPANY NAME, FIN, MISLE ID #)

I have received your letter of dd/mm/yyyy requesting designation of Public Access Facility for your location. Taking into account the provisions of these regulations that allow for certain exemptions, and after evaluating your facility, I have determined that xxxx qualifies for this designation. Your request for a PAF designation is therefore granted subject to continuing compliance with the conditions outlined below:

- Provide this office appropriate information for contacting the designated individual with security responsibilities for the Public Access Facility at all times;
- Comply with any Maritime Security (MARSEC) measures described in the Area Maritime Security Plan, all measures described in enclosure (1), and any Captain of the Port Orders requiring additional security measures, and
- Report any suspicious activities to the National Response Center at 1-800-424-8802.

As per 33 CFR part 105.110(d)(3), the Captain of the Port may withdraw the designation of a Public Access Facility at any time the owner or operator fails to comply with any requirement established as a condition of the designation, or any measure ordered by the Captain of the Port.

You must be in full compliance with the above required measures by July 01, 2004. This designation will be evaluated annually to ensure it remains appropriate. If there are any changes to the use or description of your facility you may be required to prepare and implement a Facility Security Plan in accordance with 33 CFR part 105.

I commend your continuing involvement with the Area Maritime Security Committee and the efforts you have undertaken to ensure the security of the port and the citizens of xxxxx. Please don't hesitate to contact xxx, of my staff, for any assistance.

Sincerely,

COTP Name Rank, U.S. Coast Guard Captain of the Port [insert Port Name]

Encl: (1) Required Security Measures for Public Access Facility X

Enclosure (1) List Specific
Requirements

PUBLIC ACCESS FACILITY DESIGNATION
XXXX Facility

I acknowledge and accept the conditions of the exemption from the provisions of 33 CFR part 105 documented in the Coast Guard Captain of the Port letter of xx/xx/xx. I will immediately inform the Captain of the Port of any changes of the operations at this facility that may affect this exempt status.

Signed: _____
Public Access Facility Owner/Operator

Signed: _____
Individual with Security Responsibilities

24 Hour contact information: _____

Date: _____

MTSA/ISPS POLICY ADVISORY COUNCIL

April 1, 2004

Issue/Discussion/Decision

MTSA and ISPS Tonnage Applicability

26-04

*CG-FAC Edited 2018

FINAL

Issue: What tonnages should be applied to US and foreign vessels for MTSA and ISPS applicability?

Discussion: Tonnage applicability determinations are complex, with vessel age, size, year built, IMO Convention or Amendment particulars, and Administration interpretations all impacting whether ITC or Registry tonnage can be used. For US vessels NVIC 11-93, Change 3 provides the US interpretations of the International Tonnage Convention, SOLAS applicability, and US law. For foreign flagged vessels, both US law and Administration interpretations could impact tonnage applicability determinations.

Decision: The tonnage to be applied for determining MTSA and ISPS applicability will be listed on the front of the vessel's International Tonnage Certificate, but the International Tonnage Certificate could list national (registry) tonnage as well. As such:

For US Vessels of 79 feet or greater: US national tonnage (US GRT) shall be used to determine MTSA applicability, if assigned; otherwise, use ITC tonnage. ITC tonnage shall be used to determine ISPS applicability in all cases.

For Vessels of less than 79 feet: For US vessels, US national tonnage (US GRT) shall be used to determine MTSA and ISPS applicability. For foreign vessels, national tonnage can be used to determine MTSA applicability.

For Foreign Flagged Vessels with two tonnages shown on the vessel's International Tonnage Certificate: ITC tonnage should be used to determine MTSA and ISPS applicability.

For Foreign Flagged Vessels with one tonnage shown on the vessel's International Tonnage Certificate: The tonnage reflected on the vessel's International Tonnage Certificate should be used for MTSA and ISPS applicability. The tonnage reflected on the vessel's International Tonnage Certificate should be ITC tonnage; if not, please contact CG-CVC through the Chain of Command for appropriate actions.

For US and Foreign Flagged Vessels solely navigating on the Great Lakes: For US vessels, national tonnage (US GRT), if assigned, shall be used to determine MTSA applicability. For foreign vessels, national tonnage can be used to determined MTSA applicability.

Note: For foreign vessels of 79 feet or greater, although ITC tonnage may be used for determining MTSA and ISPS applicability, national tonnage may still be used to determine some SOLAS applicability. As such, prior to initiating the application of ITC tonnage so as to change a vessel's SOLAS applicability status, please contact CG-CVC through the Chain of Command.

MTSA/ISPS POLICY ADVISORY COUNCIL

April 8, 2004

Issue/Discussion/Decision

Foreign Barges

28-04

*CG-FAC Edited 2018

FINAL

Issue: Will foreign barges, greater than 100 gross tons, be required to comply with the Maritime Transportation Security Act?

Discussion: Numerous foreign flagged barges make calls to ports throughout the United States. Questions have been raised whether such vessels are required to comply with MTSA, since barges are identified in 33 CFR 104.105(a) (8) and (9). These cites specifically require barges subject to 46 CFR Subchapters D, O, and I to comply with the regulations. No mention is made in these cites to foreign barges. However, in 33 CFR 104.105(a)(2), foreign cargo vessels greater than 100 gross tons are required to comply with MTSA. Is it our intention to require foreign barges to comply with MTSA?

Decision: The intent of 33 CFR 104.105(a)(2) was to capture the foreign flagged cargo barges greater than 100 gross tonnage. The regulations specifically define cargo, which limits the applicability to foreign vessels. Therefore, a foreign flagged cargo barge greater than 100 gross tons would be required to submit a security plan prior to operating in the U.S., unless we have some reciprocal agreement with that flag state.

MTSA/ISPS POLICY ADVISORY COUNCIL

May 13, 2004

Issue/Discussion/Decision

Lightering Operations

31-04

***CG-FAC Edited 2018**

FINAL

Issue: What is the Coast Guard's policy on vessels lightering in the Exclusive Economic Zone (EEZ) with regards to MTSA and the ISPS Code?

Discussion: The Coast Guard has historically exercised authority over vessels conducting lightering operations in the EEZ for the enforcement of pollution laws and regulations. These vessels are boarded to conduct cargo transfer monitoring when it is deemed necessary by the COTP. The following decision regards the Coast Guard's position towards security in lightering zones.

Decision: Vessels engaged in lightering operations in the marine environment, which includes the EEZ, are subject to Coast Guard regulation, when the oil or hazardous material lightered is destined for a port or place subject to the jurisdiction of the United States. Any vessel that is involved in lightering operations within the EEZ must comply with MTSA and/or the ISPS Code as applicable. (An ISPS to non-ISPS vessel interface is allowed if the non-ISPS vessel complies with MTSA in accordance with ISPS B 4.20.)

The Coast Guard has historically exercised authority over vessels conducting lightering operations in the EEZ for the enforcement of pollution laws and regulations. These vessels are boarded to conduct cargo transfer monitoring when it is deemed necessary by the Coast Guard to verify compliance with 33 CFR 156. Compliance with §156 includes maintenance of a valid Certificate of Inspection or Certificate of Compliance. In either case, compliance with the MTSA regulations and/or the ISPS Code is a required element.

The exercise of this authority is similar to the Coast Guard's policy with regard to enforcement of pollution laws and regulations. The COTP may exercise broad discretion when targeting vessels conducting lightering operations for ISPS/MTSA compliance verification and boardings will not be done routinely. However, the Coast Guard retains the authority to board any vessel lightering within the EEZ at any time to conduct a verification that all required security measures are in place, including monitoring, access control and proper Declaration of Security (DoS).

Vessels using designated lightering areas must provide 24 hours notice prior to transfer operations in accordance with 33 CFR 156.215. The COTP should screen each vessel for MTSA/ISPS compliance when the notice is received. Vessels that are not compliant with MTSA or the ISPS Code should be denied permission to use the designated lightering area.

Specific enforcement and control action for non-complaint vessels, beyond denying permission to use the designated lightering zone, are at the discretion of the COTP. If, upon reviewing the facts of a particular lightering operation, the COTP determines that it was not conducted in accordance with ISPS Code and the MTSA, the COTP may refuse entry of the servicing vessel into a port or place subject to the jurisdiction of the United States and/or deny approval to for the servicing vessel to lighter its cargo in a port or place subject to the jurisdiction of the United States.

Designated lightering areas are not affected by MARSEC level changes; however the COTP may raise the MARSEC level of any U.S. vessel that is operating in a designated lightering area if warranted.

Regulations now require ships to report such vessel to vessel activities as a last port of call.

MTSA/ISPS POLICY ADVISORY COUNCIL

June 30, 2004

Issue/Discussion/Decision

Caustic Soda Solution

33-04 Change 2

*CG-FAC Edited 2018

FINAL

Issue: Should vessels and facilities handling caustic soda solution be waived from the requirements in 33 CFR parts 104 or 105?

Discussion: Caustic Soda Solution is a bulk liquid hazardous material listed in 46 CFR Subchapter O, Table 1 to part 153. It is also considered to be a Category D Noxious Liquid Substance by MARPOL 73/78 and ships carrying this cargo are required to be certificated under 46 CFR Subchapter O. Facilities handling this product are regulated under 33 CFR 154. Under these circumstances, vessels carrying this cargo would be required to implement security plans and the facilities that receive these vessels would also have to implement security plans. Caustic soda is non-flammable and marginally toxic. The principle hazard associated with caustic soda is its corrosivity to human tissue. Due to its corrosive properties, caustic soda is inherently dangerous and may cause death, in extreme cases, to those who come into physical contact with the material. For these reasons, our transportation safety regulations (46 CFR 151 and 153) allow open venting and gauging, but require personnel involved in handling operations to be properly outfitted in chemical protective clothing. The Coast Guard Office of Design and Engineering Standards (CG-ENG) believes that caustic soda solution is not likely to cause or be involved in a transportation security incident if used maliciously.

Decision: We have conducted an assessment of caustic soda solution and have determined that it poses a lower risk of causing a transportation security incident. As a result, the Coast Guard may waive barges that handle caustic soda solution as not being subject to 33 CFR part 104 unless another applicability factor is involved. Likewise, the Coast Guard may waive facilities that receive caustic soda solution from barges not otherwise subject to 33 CFR part 104 unless another applicability factor is involved. Vessels or facilities wishing to have their operations examined in consideration for a waiver may forward a request to Commandant (CG-FAC) in accordance with 33 CFR 104.130 or 105.130. Waived barges and facilities remain subject to parts 101 and 103 of 33 CFR Subchapter H.

Barge Examples: A barge that alternates between carrying caustic soda solution and other regulated cargoes would be required to comply with 33 CFR part 104. Also, any self-propelled vessel carrying caustic soda solution and inspected pursuant to 46 CFR Subchapter I must comply with 33 CFR part 104. A barge that does not engage in international voyages that only carries caustic soda solution or other non-regulated cargoes may send a waiver request to Commandant (CF-FAC) in accordance with 33 CFR 104.130.

Facility Examples: A facility that receives any self-propelled vessel carrying caustic soda solution must comply with 33 CFR part 105. A facility that receives a barge that does not engage in international voyages that carries caustic soda solution may send a waiver request to Commandant (CG-FAC) in accordance with 33 CFR 105.130.

Inclusion in the Area Maritime Security Plan: In ports that move large amounts of Caustic Soda Solution through several waterway operators, the Area Maritime Security Plan may address mitigation strategies and implementation methods when the security of such movements are highly susceptible to suspicious activities.

MTSA/ISPS POLICY ADVISORY COUNCIL

June 3, 2004

Issue/Discussion/Decision

Locking of Public Access Facilities
34-04 Change 1

*CG-FAC Edited 2018

FINAL

Issue: Can a public access facility, such as a marina, be locked and retain public access facility status?

Discussion: This question can be answered using guidance approved by the Policy Advisory Council #24-04 Change 1. Since this guidance was released, several marinas that are regulated by 33 CFR part 105 have asked to be designated as a Public Access Facility. They would also like to use locks in order to restrict access to the facility. Can a facility restrict access to the public and still be considered a Public Access Facility?

Decision: 33 CFR 101.105 defines Public Access Facility. This definition states that such a facility is used by the public primarily for purposes such as recreation, entertainment, retail or tourism, and primarily not for receiving vessels subject to part 104.

Guidance found in the PAC 24-04 Change 1 states, "some marinas could be considered a Public Access Facility. If the marina dock receives a non-SOLAS 104 vessel, and is not subject to 33 CFR part 154, then it could meet the Public Access Facility definition. However, if the marina restricts access to their dock, then the dock does not have public access, and would not meet the definition of Public Access Facility but would be required to submit a facility security plan in accordance with 33 CFR part 105 before receiving a vessel subject to part 104."

Therefore, a facility that restricts access to the public, such as using locks at their access areas, cannot be designated as a Public Access Facility. Such facilities should not be encouraged to remove gates and locks in order to avoid the requirements of part 105. Rather, they should be instructed to submit a Facility Security Plan. This plan would explain the security operations that occur while the facility is interfacing with a vessel subject to 33 CFR part 104. When this facility is not conducting MTSA operations, it has the option to implement variable security measures (see PAC 05-03 Intermittent Operations). The facility also has the option of designating a small area within the facility that minimizes passenger interface thereby requiring security for a limited portion of that facility.

As with other waterfront business such as restaurants and shops, Public Access Facilities may have designated hours of operation. Vessels may not utilize the PAF during its non-business hours or dock for the purpose of embarking or disembarking passengers.

MTSA/ISPS POLICY ADVISORY COUNCIL

June 3, 2004

Issue/Discussion/Decision

Cruise Ships, Tenders and Public Access Facilities
35-04 Change 2

***CG-FAC Edited 2018**

FINAL

Issue: Can a designated Public Access Facility receive tenders from foreign flagged cruise ships with an approved Ship Security Plan (SSP)?

Background: 33 CFR 101.105 defines Public Access Facility (PAF) as having minimal infrastructure for receiving vessel subject to part 104 and further states that the PAF may receive only:

(i) Vessels not subject to part 104 of this chapter; or
(ii) Passenger vessels, except cruise ships, ferries certificated to carry vehicles, or passenger vessels subject to SOLAS Chapter XI.

PAFs periodically interface with cruise ships that arrive in port and anchor away from a dock. The cruise ship uses their tenders or lifeboats to ferry passengers back and forth to the dock, so that passengers may temporarily go ashore and return to the cruise ship. These lifeboats and tenders are included on the cruise ship's Passenger Vessel Safety Certificate and are considered to be SOLAS vessels.

Decision: Guidance found in Policy Advisory Council decision 24-04 states facilities that receive tenders from foreign flagged cruise vessels must be regulated under 33 CFR part 105 and must submit an FSP. Therefore, a facility that receives tenders from foreign flagged cruise vessels cannot be designated a PAF and are required to submit an FSP.

Facility Option: A PAF has the option to become a regulated facility by submitting an FSP with variable security measures for the periods of time that it is not involved in MTSA operations, see Policy Advisory Council #05-03 (Intermittent Operations). While facility owners and operators must comply with each applicable section of the regulations, the facility security assessment and plan need only mitigate the vulnerabilities associated with passenger tenders and life boat operations carrying passengers from a SOLAS vessel. These security measures may need only be applied prior to and during vessel arrivals in accordance with an approved FSP.

Foreign Flag Cruise Ship Option: The cruise ship may use U.S. flag vessels for the purposes of ferrying passengers between the PAF and the cruise ship.

MTSA/ISPS POLICY ADVISORY COUNCIL

October 26, 2004

Issue/Discussion/Decision

Shipyard Security
41-04 Change 1

*CG-FAC Edited 2018

FINAL

Issue: What security is provided in shipyards?

Discussion: 33 CFR 105.110 defines requirements to be designated as an exempted shipyard. This PAC document discusses security posture requirements for shipyards and for vessels interfacing with shipyards.

Decision: Vessel Responsibilities: An approved vessel security plan should include provisions the vessel will take when it is being received by a shipyard to include the occurrence of sea trials. Under the guidance of Navigation and Vessel Inspection Circular 04-03 Change 3, the vessel may use variable security measures for these periods when it is temporarily out of service, so long as these variable means are listed in the Vessel Security Plan (VSP).

A vessel will be considered to be without a VSP/SSP when the Flag State revokes the ISSC or COI. At this point, security of the vessel remains entirely with the shipyard. Separate agreements may be made between the vessel and the shipyard regarding security and may be based upon factors such as the extent to which the ship's personnel remain on board and retain the capability to exercise their duties. When the vessel and the shipyard need to coordinate security needs and procedures the recommended format is the Declaration of Security.

Unregulated Shipyards: The following guidance is recommended for COTPs to consider for inclusion in Area Maritime Security Plans or Facility Security Plans, where applicable, in order to reduce threats during the period when a vessel is being serviced at a ship yard.

1. Conduct a vulnerability assessment, documenting vulnerabilities on CG-Form 6025 and mitigate the identified vulnerabilities;
2. Designate someone, such as a shift supervisor or foreman, as the point of contact for security matters;
3. Designate restricted areas and institute measures to control access to these spaces;
4. Establish procedures that the shipyard would follow to report suspicious activities and breaches of security (see CG-5P Policy Letter No. 08-16), as well as transportation security incidents; consideration being given to local law enforcement authorities along with federal law enforcement authorities;
5. Document the operational hours of the shipyard and measures that it takes to control access to the property and vessels being serviced or built on the property;

6. Designate times (heightened MARSEC levels, after working hours, etc.) when visitors are not permitted on shipyard property and the protocol for the removal of such visitors, or anyone acting suspiciously;
7. Establishing procedures of how the shipyard would receive information regarding changes in MARSEC levels;
8. Establish a system by which the shipyards and vessels communicate their respective security postures and needs; the recommended format to capture such agreements is the Declaration of Security.

Regulated Shipyards: In accordance with 33 CFR 105.240, a shipyard's approved facility security plan (FSP) should include the provisions the facility will take with regards to providing security for vessels which they are receiving. Separate agreements may be made between the vessel and the shipyard regarding security and may be based upon factors such as the extent to which ship's personnel remain on board and retain the capability to exercise their duties. When the vessel and the shipyard need to coordinate security needs and procedures, the recommended format is the Declaration of Security.

Sea Trials: In accordance with the IMO/MSC Circular 1111, the security of ships undertaking sea trials is the responsibility of the State whose flag the ship is flying at the time of the trials. Therefore, the burden of security will rest with the vessel during sea trials. If the vessel is still under construction, has not been delivered, and has not yet received its ISSC or COI, then the responsibility rests with the facility to provide security.

In all cases: The attached matrix will guide those interfaces occurring between vessels and shipyard facilities.

Table 1 – Vessel security implementation at shipyards

	Shipyard, in vicinity of Vessel to Facility Interface, Requires FSP	**Shipyard Doesn't Require FSP or FSP does not Cover Vicinity of Vessel to Facility Interface**
Vessel requires VSP*	Vessel and facility fully implement security plans or coordinate vessel security needs and procedures prior to vessel arrival. Recommend use of DoS to document agreement.	Vessel security depends on provisions of VSP. Certain security measures may be taken by the shipyard to meet provisions of the Area Maritime Security Plan or other security directives and cover points listed under unregulated shipyards in this document.
Vessel does not require VSP	**Vessel Security depends on provisions of FSP.**	Certain security measures may be taken by the shipyard to meet provisions of the Area Maritime Security Plan or other security directives and cover points listed under unregulated shipyards in this document.
New Construction of vessels subject to 33 CFR part 104	Vessel security depends on provisions of FSP until vessel is delivered. At that point, vessel and facility fully implement security plans or coordinate vessel security.	Until the vessel is delivered, certain security measures may be taken by the shipyard to meet provisions of the Area Maritime Security Plan or other security directives and cover points listed under unregulated shipyards in this document. After the vessel is delivered, the security depends on provisions of VSP.

*It is recommended that a thorough sweep of the vessel be conducted prior to resuming operations to ensure no unauthorized persons or suspicious packages are onboard. It is further recommended that any vessel going into drydock be inspected, prior to refloating, for any package that may be attached.

MTSA/ISPS POLICY ADVISORY COUNCIL

October 26, 2004

Issue/Discussion/Decision

Determining Which Foreign Yachts are Subject to SOLAS

44-04

*CG-FAC Edited 2018

FINAL

Issue: With regards to foreign yachts, what does the term "subject to SOLAS" mean?

Discussion: We have received many questions from Coast Guard field units and the maritime industry regarding the applicability of MTSA/ISPS to foreign yachts. These questions have arisen in part from different interpretations of the term "subject to SOLAS." Some of the confusion has come from the differences between similar terms used in SOLAS and MTSA, which have distinct and different meanings (e.g. cargo ship in SOLAS and cargo vessel in MTSA).

MTSA and ISPS do not regulate foreign pleasure yachts. However, yachts may operate commercially. This commercial operation may subject them to ISPS.

In most cases, the vessel's flag state would have issued all required SOLAS certificates to a yacht engaged in trade, especially to a vessel carrying 12 or more passengers. That passenger ship would carry a Passenger Ship Safety Certificate and an ISSC.

Decision: A pleasure yacht not engaged in trade (i.e., is not carrying passengers for hire) is generally not subject to SOLAS, irrespective of its size, its numbers of passengers (as defined by SOLAS) or the international nature of its voyage.

The applicability section of SOLAS, Chapter XI-2 incorporates the general SOLAS applicability scheme. Although Chapter XI-2, Regulation 2, states that it applies to "passenger ships" and "cargo ships, including high speed craft, of 500 GT and upwards," these categories are modified by the general exceptions to applicability of Chapter I, Regulation 3. In other words, the general exceptions of Chapter I carry forward to the specific provisions of Chapter XI-2. Thus, a pleasure yacht not engaged in trade is not subject to the specific provisions of ISPS.

When visiting a yacht, the role of a boarding officer or marine inspector would be to determine which SOLAS documents it possesses and whether it acquired these documents voluntarily.

As a rule, a vessel that voluntarily carries one SOLAS document, such as an ISSC, but is lacking a full complement of SOLAS documents indicates that the vessel is complying voluntarily with SOLAS or portions of SOLAS. Oftentimes, owners of vessels that voluntarily carry a SOLAS document do so to prove to another nation their certification to an international standard with regards to safety equipment or security provisions. For example, a privately-owned vessel of 300 GT may voluntarily carry a Cargo Ship Safety Equipment Certificate as

evidence that it has certain lifesaving gear onboard as an alternative to complying with 46 CFR Subchapter I, as required in 46 CFR 90.05-1.

On the other hand, a vessel would need to carry a complement of SOLAS certificates in order to comply with SOLAS. These certificates could include a Passenger Ship Safety Certificate (PSSC), Cargo Ship Safety Construction Certificate (CSSCC), Cargo Ship Safety Equipment Certificate (CSSEC), Cargo Ship Safety Radio Certificate (CSSRC), Safety Management Certificate (SMC), and/or an International Ship Security Certificate (ISSC). Possessing a full complement of certificates is one important indicator that the yacht is/was at one point engaged in trade. However, there remain circumstances when owners of yachts decide to get these documents voluntarily and in these cases, the yacht would not be subject to SOLAS.

An owner cannot "turn on" or "turn off" their SOLAS documents. When a flag state determines that a vessel must meet SOLAS requirements and issues certificates verifying such conditions, the vessel must act in accordance with the documents at all times, regardless of whether the vessel is involved in trade or not.

The below examples are illustrated in an attempt to clarify this statement, and give situations where pleasure yachts are or are not "subject to SOLAS."

Example 1: A privately owned yacht engaged in trade arrives in port with a PSSC, SMC, and an ISSC. This yacht is "subject to SOLAS." The vessel would be required to moor at a facility in compliance with 33 CFR part 105 since the vessel carries the complement of certificates needed to demonstrate compliance with SOLAS.

Example 2: A privately owned yacht not engaged in trade arrives in port with a PSSC, SMC, and an ISSC. This yacht is "subject to SOLAS" because the flag state has issued certificates indicating they are authorized to engage in trade. The vessel would be required to moor at a facility in compliance with 33 CFR part 105. Despite the fact that there is no evidence that the vessel is engaged in trade, the vessel carries the complement of certificates necessary to prove that it has the intent to comply with international regulation. Steps that the vessel could take to reverse this intent would be to have the flag state remove certain documents or for the flag state to provide documentation onboard the vessel stating that the vessel is operating outside of the boundary of the certificates.

Example 3: A privately owned yacht, greater than 300 GT, not engaged in trade arrives in port with a CSSEC. This yacht is not "subject to SOLAS." The vessel would not be required to moor at a facility in compliance with 33 CFR part 105 since the vessel is in possession of a single document that only proves to the United States that it carries an equivalent amount of lifesaving equipment required by 46 CFR Subchapter I.

Example 4: A privately owned yacht, greater than 300 GT, not engaged in trade arrives in port with a CSSEC. This yacht is not "subject to SOLAS." This vessel would not be required to moor at a facility in compliance with 33 CFR part 105, as in Example 3. The fact that the vessel possesses a certificate reading "Cargo Ship" does not automatically make it a cargo vessel as defined in MTSA. MTSA defines a cargo vessel in 33 CFR 101.105 as a vessel that carries, or intends to carry any goods, wares, or merchandise for consideration. A yacht not engaged in trade would not meet the MTSA definition of cargo vessel and not need to moor at a part 105 facility.

Example 5: A privately owned yacht of 500 GT with 50 passengers onboard and engaged in trade (i.e., is carrying one or more passengers for hire) arrives in port with only a CSSEC. This yacht is "subject to SOLAS." The vessel would be required to moor at a facility in compliance with 33 CFR part 105 since the vessel meets the applicability of SOLAS as a passenger vessel. It is anticipated that the COTP would be able to identify port call non-compliance with 33 CFR Chapter I, Subchapter H before the vessel's mooring, since vital information will be provided through the Notice of Arrival regulations in 33 CFR part 160. When the vessel moors, the COTP should also investigate the reasons the vessel does not carry a PSSC, ISSC, and SMC.

Example 6: A privately owned yacht, greater than 300 GT, not engaged in trade arrives in port with only an ISSC. Upon investigation, the Master reveals that the vessel carries this document on a voluntary basis, due to his concerns of international security threats. This yacht is not "subject to SOLAS." This vessel would not be required to moor at a facility in compliance with 33 CFR part 105 since the vessel obtained the certificate voluntarily. The COTP may need to investigate the reasons the vessel does not comply with 46 CFR 90.05-1 and carry a COI or CSSEC.

Example 7: A privately owned yacht, greater than 300 GT, not engaged in trade arrives in port with an ISSC and CSSEC. The yacht obtained the CSSEC in order to meet the requirements of 46 CFR Subchapter I. It obtained the ISSC when reading the applicability of ISPS and believing that the Code was applicable to vessels not engaged in trade. Learning that the applicability of ISPS mimics the applicability of SOLAS, the Master learns that he is not required to possess the ISSC, but voluntarily decides to maintain its provisions. This yacht is not "subject to SOLAS." As in Example 6, this vessel would not be required to moor at a facility in compliance with 33 CFR part 105 since the vessel obtained the certificates voluntarily.

Example 8: A privately owned yacht of 200 GT and not engaged in trade arrives in port with no SOLAS documents. This yacht is not "subject to SOLAS." MTSA regulations would not require the vessel to moor at a facility in compliance with 33 CFR part 105. This vessel is not subject to 46 CFR Subchapter I, since it is not a motor, sea-going vessel greater than 300 GT.

Example 9: The owner of a privately owned yacht provides his vessel to a charter party [Time or Voyage charter]. At the time of the charter, the yacht carries the complement of documents necessary to determine that it is "subject to SOLAS". Since the charter is a bareboat charter, the vessel would not maintain the status of being "subject to SOLAS." The yacht would not need to moor at facilities in compliance with 33 CFR part 105 for the duration of the charter. At the end of the charter and the return of the yacht to the original owners, the yacht would return to a "subject to SOLAS" designation.

Example 10: The owner of a privately owned yacht provides his vessel and a crew to a charter party [Time or Voyage charter]. At the time of the charter, the yacht carries the complement of documents necessary to determine that it is "subject to SOLAS." Since the charter is not a bareboat charter, the vessel would maintain the status of being "subject to SOLAS." The yacht would need to moor at facilities in compliance with 33 CFR part 105 for the duration of the charter, as well as periods before and after the charter.

MTSA/ISPS POLICY ADVISORY COUNCIL

November 8, 2005

Issue/Discussion/Decision

Timelines for MTSA Required Exercises

45-04 Change 2

*CG-FAC Edited 2018

FINAL

Issue: When should the first MTSA exercise be conducted?

Discussion: Vessel and facility exercises, as defined in 33 CFR 104.230, 105.220 and 106.225, must be conducted at least once each calendar year, with no more than 18 months between exercises. The regulations did not specify when the first exercise would be conducted.

Area Maritime Security Plan exercises required by 33 CFR 103.515 are to be performed at least once each calendar year, with no more than 18 months between exercises.

Realizing that some plans are approved well in advance of the actual date the vessel or facility would commence operations, additional guidance is necessary that allows a vessel or facility to have available the full 18 month time period by which to conduct the required exercises.

Decision: An exercise must be conducted no later than 18 months from the first day of commencement of operations, otherwise referred to as the plan implementation date.

If a vessel or facility chooses to conduct an exercise at the end of the 18 month window as allowed for, the next required annual exercise compliance date ***cannot*** again be deferred for another 18 months. Exercises are required to be conducted once per calendar year.

MTSA/ISPS POLICY ADVISORY COUNCIL

December 7, 2004

Issue/Discussion/Decision

Capability to Continuously Monitor

48-04

*CG-FAC Edited 2018

FINAL

Issue: What is the interpretation of the phrase "capability to continuously monitor" as used in 33 CFR 104.285, 105.275 and 106.275?

Discussion: The Preamble to the Final Rule (October 22, 2003, page 60496) defines the term "continuously monitor" to mean that vessel and facility owners must always be capable of monitoring. Application of this definition has resulted in different security postures being applied in COTP zones. In one zone, facilities are being required to monitor all portions of their property 24 hours a day. In another, facilities are left unoccupied overnight and not being monitored, but these facilities have contracted security agents in cases where more security is needed.

Decision: Vessels and facility owners are not required to provide continuous monitoring, per 33 CFR 104.285, 105.275 and 106.275. These requirements state that the vessel and facility have the ***capability*** to continuously monitor, which does not mean that they have to monitor at all times. Rather, it is anticipated that the vessel or facility would employ the capability to monitor the facility when MARSEC Levels are increased.

In cases where an FSP or VSP require continuous monitoring at all MARSEC Levels, that vessel or facility must meet those standards – this document will **NOT** supersede anything written in an approved security plan. Vessels or facilities that would like to change their plans to incorporate this interpretation must follow guidance found in 33 CFR 104.415, 105.415 or 106.415 and submit required plan amendments.

MTSA/ISPS POLICY ADVISORY COUNCIL

January 18, 2005

Issue/Discussion/Decision

Urea Ammonium Nitrate Solution (2% or less NH_3)

51-05

*CG-FAC Edited 2018

FINAL

Issue: Should vessels and facilities handling Urea Ammonium Nitrate (2% or less NH_3) be waived from the requirements in 33 CFR part 104 or 105?

Discussion: UAN solution that contains 2% or less NH_3 is classified as a category D noxious liquid substance by MARPOL regulations. 33 CFR 154 applies to any cargo that is listed as a category D noxious liquid substance. 33 CFR 154 does not limit its applicability to facilities receiving vessels subject to MARPOL and therefore, a facility handling UAN solution that contains 2% or less NH_3 is subject to 33 CFR 105. The Coast Guard Hazardous Materials Standards Division (CG-ENG) believes that Urea Ammonium Nitrate (2% or less NH_3) is not likely to cause a transportation security incident even if used maliciously.

Decision: We have conducted an assessment of Urea Ammonium Nitrate (2% or less NH_3) and have determined that it poses a lower risk of causing a transportation security incident. Therefore, facilities or vessels wishing to have their operations examined in consideration for a waiver may forward a request to Commandant (CG-FAC-2) in accordance with 33 CFR 105.130 or 33 CFR 104.130.

Vessel Examples: A barge that alternates between carrying Urea Ammonium Nitrate (2% or less NH_3) and other regulated cargoes would be required to comply with 33 CFR part 104. Also, a self-propelled vessel carrying Urea Ammonium Nitrate (2% or less NH_3) that is greater than 100 gross register tons and inspected pursuant to 46 CFR Subchapter I must comply with 33 CFR part 104. A barge that does not engage on international voyages that carries only Urea Ammonium Nitrate (2% or less NH_3) or other non-regulated cargoes may request a waiver as described above.

Facility Examples: Facilities that receive vessels over 100 gross tons that are inspected pursuant to 46 CFR Subchapter I or facilities that receive vessels on international voyages are examples of facilities that must meet the requirements of 33 CFR part 105, even though the only cargo they handle is Urea Ammonium Nitrate (2% or less NH_3). A facility that receives a US vessel carrying only Urea Ammonium Nitrate (2% or less NH_3) may request a waiver as described above.

Inclusion in the Area Maritime Security Plan: In ports that move large amounts of Urea Ammonium Nitrate (2% or less NH_3) through several waterway operators, the Area Maritime Security Plan may address mitigation strategies and implementation methods when the security of such movements are highly susceptible to suspicious activities.

MTSA/ISPS POLICY ADVISORY COUNCIL

March 7, 2005

Policy

Towing vessels moving regulated barges NOT carrying CDCs

53-05

*CG-FAC Edited 2018

FINAL

Issue: Are U.S. towing vessels engaged in towing barges subject to part 104 required to have a vessel security plan (VSP) if the barge is not actually carrying a regulated cargo such as a CDC in bulk?

Discussion: The temporary final rule in federal register, August 18, 2004, changed 33 CFR parts 104, 105 and 160. In doing so, it inadvertently captured a segment of the marine industry that was not intended to be captured.

Prior to this rule change applying to CDCs, barges inspected under subchapter I that carry CDC in bulk were subject to part 104. This meant that towing vessels engaged in towing these barges were also subject to part 104 and required to have a VSP.

This rule change also meant that all barges (inspected and uninspected) that carry CDC in bulk were subject to part 104. Therefore, every towing vessel engaged in pushing or pulling these barges is subject to part 104. This exponentially increased the number of towing vessels required to have a VSP.

The Coast Guard's policy is that if a vessel is subject to part 104 they are always subject to part 104 no matter what they are carrying. When a vessel security plan is submitted and approved, the vessel will be expected to operate in accordance with the VSP at all times unless the VSP is withdrawn. VSPs may not be turned off when carrying non-regulated cargoes and back on before carrying regulated cargoes. The VSP may contain variable security measures to cover multiple operating conditions but the security plan must always be implemented.

The significance of this rule change is that now, every towing vessel engaged in towing these barges, no matter what cargo the barge is carrying (sand, rock, grain…), is required to have a VSP. Many of these towing vessels have no intention of ever towing a barge with a regulated cargo. As such, many companies did not interpret the "subject to this part" in 33 CFR 104.105(a)(11) the same way as the Coast Guard and never submitted a VSP.

This rule change specifically affects the movement of Ammonium Nitrate (AN). AN is an essential product used in the farming industry but represents less than 1% of the barge movements by covered dry cargo barges. Since the number of movements is so few, it is not cost effective to have dedicated barges to move this product. The industry is willing to implement and maintain security plans on a group of their barges (1500+/-) so that when they receive a call to move a shipment, they can use their closest regulated barge and not have to wait

for a specific barge to arrive. However, it would be a financial burden on the industry if every towing vessel that ever moved these barges were required to have a VSP.

When the regulations were written, towing vessels moving unregulated cargoes were not intended to get swept up in the part 104 applicability. The compliance section for facilities in the federal register, August 18, 2004, only applies to facilities receiving vessels carrying AN. We are requesting the same exemption for towing vessels.

Policy: In interpreting 33 CFR 104.105(a)(11) only, a barge or barges subject to this part does not include "uninspected barges during instances that they are not carrying a CDC in bulk."

The effect of this is when an uninspected barge is not carrying a CDC in bulk, such as AN, a towing vessel moving it will not be required to have a VSP, provided that there is no other basis that would require such a vessel to have a plan.

MTSA/ISPS POLICY ADVISORY COUNCIL

April 26, 2005

Policy

Exceptions to part 105 Applicability for Oil and Natural Gas Facilities

57-05

*CG-FAC Edited 2018

FINAL

Issue: Clarification has been requested with respect to the exceptions provided for by 33 CFR 105.105(c)(2) and (3).

1) Do the exceptions stated in 33 CFR part 105.105(c) override applicability factors stated in part 105.105(a)?

2) If an excepted facility interfaces with a vessel subject to 33 CFR part 104 will the facility lose the exception and become subject to 33 CFR part 105?

3) Is there a requirement that both the facility and the vessel(s) that it interfaces with be under the same ownership?

4) Are vessels that are otherwise subject to 33 CFR part 104, who call solely on these excepted facilities, excused from the requirements of 33 CFR part 104 as well?

5) May facilities that receive ISPS certified foreign flagged vessels engaged on international voyages claim this regulatory exception?

6) May facilities that receive non-MTSA or non-ISPS regulated foreign flagged vessels claim this regulatory exception.

Discussion: 33 CFR 105.105(c)(2) provides exception to the regulation for certain facilities i.e. "An oil and natural gas production, exploration, or development facility regulated by 33 CFR parts 126 or 154 if (i) The facility is *engaged solely* in the exploration, development, or production of oil and natural gas; and (ii) The facility does not meet or exceed the operating conditions in 106.105 of this subchapter . . ."

33 CFR 105.105(c)(3) provides exception to the regulation for certain facilities i.e. "A facility that supports the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 if (i) The facility is *engaged solely in the support* of exploration, development, or production of oil and natural gas and transports or stores quantities of hazardous materials that do not meet or exceed those specified in 49 CFR 172.800(b)(1) through (b)(6); or (ii) The facility stores less than 42,000 gallons of cargo regulated by 33 CFR part 154 . . ."

The above referenced regulations describe specific criteria that facility owners and/or operators and Coast Guard personnel must be attentive to when consideration is being given to excepting a facility from regulation under 33 CFR part 105.

Through this policy, we are clarifying the exceptions provided in 33 CFR 105.105(c). We are also clarifying our regulatory posture for facilities that receive Offshore Supply Vessels (OSVs) certificated under Subchapters I and L. Facilities that receive OSVs certificated under Subchapter L are not required to have part 105 Security Plans. Since OSVs certificated under Subchapter L are essentially identical to those certificated under Subchapter I, a similar posture is felt to be adequate for facilities that receive both types of OSVs. Facilities receiving these OSVs that are not subject to 33 CFR part 126 or 154 cannot meet the regulatory exception in part 105.105(c) and should submit waiver requests which will be considered on a case-by-case basis.

Policy:

1) Facilities that receive foreign vessels subject to SOLAS Chapter XI *may not* claim an exception from regulation as allowed in 33 CFR 105.105(c).

The exceptions described in 33 CFR 105.105(c)(2) and (3) may be allowed only when a facility meets *all* of the criteria enumerated; with the operative words for exception being: *"engaged solely in . . ."*

Facility owners or operators and Coast Guard personnel, must ensure that when applying exception criteria a facility's operations *cannot include regulated activities outside or in addition to those described in the criteria for exception, included "engaged solely in . . ."*

For example: a facility would not be allowed to claim or continue exception from regulation if it engaged in any regulated activity not associated with being *"solely engaged in . . ."* oil and natural gas operations as described in regulation i.e. exploration, development and production.

On the other hand, a facility, meeting all provisions of the section 105.105(c)(3) exception, that receives U.S flagged OSVs, which solely support oil and gas operations, would not need to meet the requirements of 33 CFR part 105. Facilities covered under this exception could receive any of the following vessels, among others: U.S. flagged OSVs certificated under Subchapter L or Subchapter I and U.S. Flagged OSVs carrying SOLAS documents.

Once a facility fully meets the criteria for exception from regulation, and maintains such qualification, only then would such exception override applicability factors in 33 CFR 105.105, unless the facility receives foreign vessels subject to SOLAS Chapter XI.

Facilities that do not qualify for this exception may request waivers, as described in 33 CFR 105.130. Facilities, such as those not subject to 33 CFR parts 126 and 154, and those operating outside of oil and natural gas business, are encouraged to follow the waiver procedures outlined in 33 CFR 105.130.

2) No. A facility may interface with a vessel subject to 33 CFR part 104 and maintain exception from 33 CFR part 105 as long as the interface is related to activities that *are "solely engaged in . . "* oil and natural gas operations as described in regulation**.**

3) No. There is no requirement that excepted facilities and the vessels that call on them be under the same ownership.

4) No. Vessels otherwise subject to 33 CFR part 104 who call solely on excepted facilities remain subject to the applicable provisions of 33 CFR part 104.

5) No. The U.S. obligations as a signatory of the International Ship and Port Facility Security (ISPS) Code requires port facilities serving vessels with International Ship Security Certificates engaged on international voyages to comply with the Code. Therefore, facilities receiving ISPS certified foreign flagged vessels engaged on international voyages are not able to claim this regulatory exception and must comply with 33 CFR part 105.

6) Yes. As long as the facility meets the criteria outlined in 33 CFR 105.105(c), it may claim the exception.

MTSA/ISPS POLICY ADVISORY COUNCIL

August 16, 2005

Policy

Facilities and Vessels Receiving Exercise Credit for Participating in Area Maritime Security Plan Exercises

59-05

***CG-FAC Edited 2018**

FINAL

Issue: Can Facility and Vessel owners or operators participate in Area Maritime Security (AMS) Plan exercises to satisfy MTSA annual exercise requirements?

Discussion: Maritime facilities with approved Facility Security Plans (FSP) under 33 CFR part 105.220 and Vessels with approved Vessel Security Plans (VSP) under 33 CFR 104.230 are required to perform annual exercises that adequately prepare the Facility/Vessel Security Officers (FSO/VSO) and Personnel/Crewmembers to respond to threats they are most likely to encounter. Exercises must be conducted at least once each calendar year with no more that 18 months between exercises. They must test the proficiency of personnel in assigned security duties at all Maritime Security (MARSEC) Levels, the effective implementation of the Plans and identify any security related deficiencies needing to be addressed.

Policy: MTSA Security Plan holders may satisfy mandated exercise requirements by voluntary and substantial participation in a U.S. Coast Guard Captain of the Port (COTP) sponsored AMS Plan exercise when one is scheduled in their area.

Exercises must be designed to be Facility or Vessel specific, or part of a cooperative exercise program that exercises applicable facility and vessel security plans, or comprehensive port exercises.

The exercise should validate the adequacy of:

1) Response to changes in MARSEC Levels;
2) Procedures for interfacing with facilities and other vessels;
3) Declarations of Security (DoS);
4) Communications;
5) Security measures for access control;
6) Security measures for restricted areas;
7) Security measures for handling cargo;
8) Security measures for delivery of vessel stores and bunkers;
9) Security measures for monitoring; or
10) Security incident procedures.

MTSA mandates records of exercises must be retained by the FSO/VSO for U.S. Coast Guard review for a period of two (2) years. Records should include the date the exercise was held, a description of the exercise, a list of participants and any best practices or lessons learned which may improve the FSP.

If no AMS Plan exercise is scheduled by the U.S. Coast Guard COTP for their area within the period that the annual exercise of their FSP/VSP plan is required, owner/operators with an approved FSP/VSP must design and execute an exercise of their own or participate in a group exercise under the auspices of another industry, port authority or governmental group.

Exercises of MTSA FSPs/VSPs are self-evaluated and self-credited; therefore, provide broad latitude to plan holders in establishing how they can best test the functional adequacy of their security plan.

Plan holders may take credit for having performed the exercise if all objectives of the exercise are met, the exercise is evaluated, and a proper record is generated. In order for an exercise to meet the intent of the regulations under MTSA the minimum requirements are that the exercise must be a full and comprehensive test of the facilities/vessels communication ability, notification procedures, elements of coordination, resource availability and response in the event of an incident.

Plan holders with an approved FSP covering more than one facility as allowed in 33 CFR part 105. 410(d) and plan holders with an approved VSP covering more than one vessel wherein the design and operations are similar as provided in 33 CFR 104.410(d) and (e) are required to conduct one exercise for the total plan with each covered facility/vessel exercising the facility/vessel-specific sections relevant to notification, communication and response to the exercised incident.

MTSA/ISPS POLICY ADVISORY COUNCIL

September 9, 2005

Policy

US Flagged Small Passenger Vessels with SOLAS Documents

60-05

*CG-FAC Edited 2018

FINAL

Issue: In addition to using facilities which are regulated by 33 CFR part 105, what options are available for US flagged Small Passenger Vessels (SPV) that carry SOLAS documents?

Discussion: Numerous marinas, commercial piers, fueling docks, public landings, and small floating docks receive U.S. SPVs inspected under Subchapter T. If the SPV only travels domestically and therefore is not subject to SOLAS, the facility is not regulated under 33 CFR part 105. However, there are a number of vessels that usually travel on domestic routes, but carry SOLAS documents allowing the vessel to make international voyages. In most cases, these vessels would not be regulated by MTSA aside from the fact that they have SOLAS documents onboard. By the terms of the regulations facilities that receive these SOLAS documented vessels must comply with 33 CFR part 105 or they must be covered by an approved waiver.

U.S. vessels with International Ship Security Certificates (ISSC) that stop at facilities in U.S. ports or places on a voyage to or from a port or place in a foreign country are on an international voyage and are subject to SOLAS. Facilities that receive these vessels must comply with 33 CFR part 105, as per 33 CFR 105.105(a)(3). This policy focuses on options available for U.S. flagged SPVs through the waiver process. This policy does not apply to foreign flagged SOLAS vessels.

The policy regarding whether SPVs with SOLAS documents on domestic voyages would need to use facilities regulated by 33 CFR part 105 has been through many iterations. This subject was debated because the definition of domestic voyage was never provided. These debates eventually caused Issue Paper 27-04 to be withdrawn. Policy Advisory Council Document (PAC) #60-05 now removes the term domestic voyage and clarifies our interpretation of the regulations.

This PAC document is intended to clarify our interpretation of the regulations with respect to U.S. SPVs operating point to point between U.S. port facilities and on those occasions when they engage on international voyages. A Compliance and Enforcement Working Group convened in Victoria, BC on June 7-8, 2005. This group was comprised of Transport Canada, USCG Headquarters and CG District representatives. The working group agreed upon the concepts expressed in this policy. Members of this group recommended that the Coast Guard begin negotiations with Canada to amend the US/Canadian Alternative Security Arrangement.

Policy: Owners or operators of U.S. SPVs (vessels certificated to carry 150 passenger or less) that carry SOLAS documents must request a waiver from the requirement to use U.S. facilities regulated by 33 CFR part 105. Any owner or operator of an SPV that carries SOLAS documents is eligible for this waiver. Waiver requests must be submitted in writing with justification to Commandant (CG-FAC) in accordance with 33 CFR 104.130.

Commandant's response to waiver requests will state that the SPV must absorb the security requirements normally performed by the facility including increasing the amount of passenger and baggage screening and implementing security measures for the current MARSEC Level in accordance with their Vessel Security Plans (VSPs). SPVs remain responsible for meeting the requirements of MARSEC Directives 104-1 and 104-2 for those passengers re-boarding the vessel during port calls and communicate with the Captain of the Port (COTP) in the regions in which they are planning to operate under this alternative policy. Prior to departing for a foreign port, and when first returning from a foreign port, the SPV must moor at a 33 CFR part 105 compliant facility.

When applying the guidance of this policy, the definition of what constitutes a voyage is critical. The definition of voyage is "the vessel's entire course of travel, from the first port at which the vessel embarks passengers until its return to that port or another port where the *majority* of the passengers disembarks and terminates their voyage."

The categories of vessels that are eligible to request this waiver include:

(1) U.S. Flagged SPVs engaged on international voyages to Canada with passengers for hire;
(2) U.S. Flagged SPVs engaged on international voyages to other countries with no passengers for hire; and
(3) U.S. Flagged SPVs engaged on non-international voyages with passengers for hire (while engaged on these non-international voyages, the vessel chooses to keep SOLAS documents onboard the vessel.)

Generally, the response to vessels asking for this waiver will include the following provisions:

(1) This waiver applies in U.S. waters when the vessel is engaged on an international voyage between U.S. and Canadian ports or marine facilities or when the vessel is on a non-international voyage;
(2) The first marine facility that receives the vessel when arriving from a foreign port or marine facility must be a 33 CFR part 105-regulated facility;
(3) The last marine facility that receives the vessel prior to departing for a foreign port or marine facility must be a 33 CFR part 105-regulated facility;
(4) At the port of embarkation all unaccompanied baggage and passengers, along with their baggage and personal effects, must be screened either by a 33 CFR part 105-regulated facility or by the vessel;
(5) All other facilities that receive the vessel when it is operating in the United States do not need to be regulated by 33 CFR part 105. This category includes facilities that interface with vessels dropping passengers off to sightsee, visit restaurants, shop, etc. Before the facility can be used, either the vessel or the facility must notify the Captain of the Port (COTP) in writing at least 30 days prior to the vessel's arrival and must include a copy of their waiver letter in the notification package. The COTP must be notified immediately of any changes to the submitted schedule;

(6) While interfacing with a non-33 CFR part 105-regulated facility the vessel must implement security measures for the current MARSEC level in accordance with its Vessel Security Plan. This policy does not excuse vessels from their requirement to screen passengers at port calls following their initial embarkation in accordance with MARSEC Directives 104-1 and 104-2 (i.e. a certain percentage of persons, baggage, and personnel effects would be screened after the passengers rejoin a vessel after eating dinner at a shore-side establishment).

In cases where the VSP requirements differ from what is expressed in this policy, the more stringent provisions shall be implemented.

TWIC/MTSA POLICY ADVISORY COUNCIL

November 21, 2007

Policy
TWIC & Law Enforcement Officials & Other Regulatory Agencies
01-07

Issue (01-07) – 33 CFR 101.514 refers to "law enforcement officials" as not being required to obtain a TWIC to access secure areas of regulated vessels or facilities. Further guidance as to who qualifies as a "law enforcement official" for the purposes of TWIC requirements is required. Additionally, fire department officials routinely access facilities as part of their regulatory inspection duties. Will fire department officials be required to obtain a TWIC or be escorted when conducting this function?

Background – 33 CFR 101.514(c) states that "law enforcement officials at the State or local level, are not required to obtain or possess a TWIC to gain unescorted access to secure areas. NVIC 03-07 states "State and local law enforcement officials may use this exemption in the course of their official duties." Further guidance as to what constitutes a law enforcement official for exemption purposes has been requested. Specifically, do State environmental officials and others with regulatory enforcement responsibilities at the State and local level qualify?

Discussion – We consider a law enforcement official for the purpose of TWIC to be any officer or employee of any agency or authority of the United States, a State, a commonwealth, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

Investigate or conduct an official inquiry into a potential violation of law; or

Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law;

and is doing so while acting in their official capacity.

State environmental officials and others with regulatory enforcement responsibilities at the State and local level who meet these criteria are not required to obtain a TWIC to gain unescorted access. However, they may voluntarily obtain a TWIC.

State and municipal fire departments and their officials who require access to secure areas of MTSA facilities for regulatory inspections in conjunction with their official duties fall within the definition given above, and as such are ***not*** required to obtain a TWIC or be escorted, as they are considered law enforcement officials. However, they may voluntarily obtain a TWIC.

TWIC/MTSA POLICY ADVISORY COUNCIL

November 21, 2007

Policy

Escorting aboard U.S. Flagged Vessels Operating in Foreign Waters

02-07

Issue (02-07) – What are the acceptable escorting standards for U.S. vessels operating in foreign waters?

Background – 33 CFR 104.265 requires that individuals who do not have a TWIC be escorted, as defined in 33 CFR 101.105, at all times while inside a secure area of the vessel. 33 CFR 101.105 defines "escorting" as "ensuring that the escorted individual is continuously accompanied while in a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted." The definition elaborates that this can be accomplished through side-by-side accompaniment or via monitoring, depending upon where the escorted individual is granted access.

Discussion – U.S. vessels operating in foreign waters face considerable challenges when implementing the TWIC program. Foreign port workers will likely not have TWICs, and as a result, they would need to be escorted every time they step aboard the vessel. This presents operational difficulties, as there are not likely to be sufficient vessel personnel onboard to escort the port workers in the ratios described in NVIC 03-07.

These vessels are required, under 33 CFR 104.265, to control access to the vessel (in a general fashion, in addition to requiring TWICs). These access control methods should already be included in the vessel's security plan, and they should include methods and/or security measures for ensuring, for example, that foreign port workers do not access restricted areas unless absolutely necessary (33 CFR 104.270(a)), and that foreign port workers are not able to introduce dangerous substances or devices onboard the vessel(33 CFR 104.265(a)). Thus, U.S. vessels operating in foreign waters shall be deemed to be properly "escorting" individuals who do not hold a TWIC when operating in accordance with the U.S. Coast Guard approved vessel security plan. This interpretation ONLY applies, however, when the vessel is operating in foreign waters.

TWIC/MTSA POLICY ADVISORY COUNCIL

January 7, 2008

Policy

Redefining Secure Areas and Acceptable Access Control

01-08

Issue (01-08) – If certain mixed-use Maritime Transportation Security Act (MTSA) regulated facilities are permitted to redefine their secure area for TWIC purposes, what guidelines should Coast Guard Captains of the Port (COTP) and regulated facilities use to assist in their redesignation decisions? What measures will be expected/accepted by the Coast Guard for access control to these newly defined secure areas?

Background – Title 33, U.S. Code of Federal Regulations, §105.115 (33 CFR 105.115) permits owners/operators of certain facilities to redefine their secure areas for TWIC applicability purposes. The Coast Guard's Navigation and Vessel Inspection Circular (NVIC) 03-07 further describes the Coast Guard's interpretation of that regulation. The NVIC permitted owners/operators of facilities with significant non-maritime related portions to exclude those non-maritime portions from the requirement for persons needing unescorted access to possess a TWIC. That provision in the NVIC has spawned questions on how much of the previously included facility area can be excluded through redesignation. Further, there has been confusion regarding the application of the redesignation option, which may lead to inconsistency between COTP zones. In some cases all MTSA regulated facilities may be incorrectly accorded the redesignation option, not just those with significant non-maritime related portions. In others, those that may be eligible may not be accorded this option. This would not be in line with the regulation, nor with the Coast Guard's intention in issuing the regulation.

Once redesignation is authorized, 33 CFR 105.255(a)(4) stipulates that the facility owner or operator must ensure implementation of security measures to prevent an unescorted individual from entering an area of the facility that is designated as a secure area, unless the individual holds a duly issued TWIC, and is authorized to be in the area. NVIC 03-07, further states that the redefined area must have sufficient access control measures such as fencing, gates, monitoring, etc., in order to deter and restrict unauthorized persons from gaining access to the secure area.

Discussion – 33 CFR 105.115(c) states "Facility owners or operators wishing to designate only those portions of their facility that are directly connected to maritime transportation, or are at risk of being involved in a transportation security incident as their secure area(s), must do so by submitting an amendment to their Facility Security Plan to their cognizant COTP." Determining whether to approve these amendment requests is essentially a 3-step process.

Step 1: Does the facility have a significant non-maritime transportation related portion?

If the answer is yes, proceed. If the answer is "no", deny the request.

First, NVIC 03-07 limits the opportunity for amendments to redefine the secure areas to "those facilities with a significant non-maritime transportation component". It goes further to state, "Amendments to redefine the secure area for other facilities and for vessels *will not be considered*" (emphasis added). And, further provides explanations of typical non-maritime transportation components. They include, but are not limited to:

- Refineries
- Chemical plants
- Factories
- Mills
- Power plants
- Smelting operations
- Recreational boat marinas
- Public areas of Passenger Vessel Facilities(Not mentioned specifically in NVIC 03-07 but added for clarity)

Step 2: Is the area to be excluded non-maritime transportation related?

If the answer to that question is no (i.e. if it is SOLELY maritime transportation related), then you go no further and you deny the request.

If the answer to that question is "yes" (i.e. if it is SOLELY non-maritime transportation related), then you go no further and you approve the request.

If the answer is "yes and no" (i.e. if it is both maritime and non-maritime transportation related -- using the NVIC example of a coal

pile supplied by a vessel but used by the power plant), then you go to the next step:

Step 3: Is the area to be excluded at risk of a TSI?

The answer to this portion will always be facility specific and require the facility owner/operator and the COTP to exercise his/her professional judgment regarding the potential for a transportation security incident upon the maritime related portion of the facility.

33 CFR part 6.01-4[1] provides a narrow designation of a waterfront facility that certain owner/operators may find appealing, as it would leave much of the MTSA regulated facility outside of this definition of "waterfront facility", and thus able to be excluded from the secure area. This however, would exclude from the secure area many portions of the facility at risk of a transportation security incident (TSI), and therefore not an acceptable alternative. The potential for a TSI is the critical component of the extent of redesignation question if you are dealing with a portion of the facility that serves both maritime and non-maritime related functions. Part of this determination lies in the location of the area to be excluded with respect to the waterfront, i.e. its proximity to the waterway and the hazards of the cargo being stored. The aforementioned factors should be analyzed concurrently and the risk of a TSI given the highest priority.

Per 33 CFR 101.105, a transportation security incident is a security incident resulting in a significant:

- loss of life,
- environmental damage,
- transportation system disruption, or
- economic disruption in a particular area

Key to the determination on whether proposed redesignations of secure area are appropriate is the understanding of what is meant by the TSI components. Once the parameters of those components are understood, the facility owner/operator and COTP can use his/her judgment to analyze whether proposed excluded portions of the facility could reasonably cause a TSI. If they can't, the redefinition should be approved. If those portions could cause a TSI, the COTP is right to reject the facility owner/operator's submission or ask for a differently defined secure area.

[1] 33 CFR 6.01-4 defines a waterfront facility as "all piers, wharves, docks, or similar structures to which vessels may be secured and naval yards, stations, and installations, including ranges; areas of land, water, or land and water under and in immediate proximity to them; buildings on them or contiguous to them and equipment and materials on or in them"

In general, COTPs can use the expanded discussions of the TSI components (found in the MTSA temporary interim rules at 68 FR 39243 – 39250 July 1, 2003)[2], to help establish redesignation boundaries. COTPs should be able to conclude whether the part of a facility that is proposed to be excluded contains bulk liquid cargo storage, oil or hazardous material that could pollute navigable waterways. COTPs should be able to assess the potential that a proposed to be excluded part of a facility has for experiencing over 150 deaths. While principally designed with passenger or port worker deaths in mind, consideration may need to be given to surrounding population areas.

Economic disruption and transportation system disruption are more difficult to consider, since the regulatory preamble didn't discuss them. In general, the facility's criticality to the area/region must be considered in analyzing the appropriateness of excluding portions of the facility for TWIC purposes. A COTP should evaluate things like another transportation mode's loading rack in the context of its area criticality. Would the loss of that distribution point remove the ability to move that cargo in the area, or are there other redundant capabilities in the area? Is there other transportation mode infrastructure proposed to be excluded that, if destroyed, would seriously impact regional rail transportation? Are there proposed to be excluded bridges over barge channels that would render that route unusable with no easy alternative route? Are there potential catastrophic explosive materials that are located in a newly excluded area that if detonated would result in channel/harbor closure for an extended period of time?

Policy - The intent of this provision is to allow owners/operators to exclude from the secure area those areas within their facility that would not have been required to be part of the original facility security plan, but were included by owners/operators for their own reasons (usually convenience, to avoid having to fence off an area of their property and institute a new access control location). Typically, these areas include refineries, chemical plants, factories, mills, power plants, smelting operations, or recreational boat marinas. As stated in NVIC 03-07, commercial docks, container yards, passenger terminals, and storage areas or tank farms that are specifically used to stage cargo for loading to a vessel or to receive cargo at its first point of rest upon discharge from a vessel (NVIC 03-07) should be considered as

[2] 68 FR 39243 – 39250 July 1, 2003 can be found on http://homeport.uscg.mil under: missions – maritime security – TWIC – general information.

having a maritime transportation nexus, and therefore are ineligible for exclusion from the secure area.

Owners or operators of facilities regulated under 33 CFR part 105 may choose to redefine their secure areas, but only where they have significant non-maritime related portions. The redefinition is limited to excluding from the secure area those portions of their facility with a non-transportation based function. This would mean that the TWIC provisions of part 105 no longer apply to those portions. Owners or operators may also choose to maintain their secure area as the entirety of the area defined in their original Facility Security Plan (FSP).

COTPs will adhere to the guidance in NVIC 03-07 regarding which facilities are eligible for redesignation of their secure areas for TWIC purposes. Area and district commanders will ensure consistency of application among COTP zones. For appropriate requests for redesignation (i.e. those pertaining to non-maritime security related portions of the facility), COTPs will analyze the potential for the excluded portions to cause a TSI. The explanation in the Discussion section above regarding TSI component thresholds will be considered in the COTP analysis.

Owners/operators of facilities are expected to meet the requirement to control access to those newly redesignated secure areas by the use of any measures that, alone or in combination, will prevent access by individuals not in possession of a TWIC or by TWIC holders who do not have an authorization for unescorted access.

Methodology for access control remains unchanged. Owners/operators might utilize fencing, gates, CCTV, roving patrols, any other recognized access control measure or any combination of measures that accomplished the performance based standard, i.e. *preventing* unescorted access to secure areas by non-TWIC holders or unauthorized TWIC holders. In determining the appropriate level of access control to the redefined secure areas of regulated facilities, the Facility Security Assessment (FSA) should be reviewed to make sure all access control provisions properly address the vulnerabilities and risks identified.

TWIC/MTSA POLICY ADVISORY COUNCIL

January 25, 2008

Policy
Federal & Law Enforcement Officials Authority to act as Escorts on Regulated Facilities and Vessels
02-08

Issue (02-08) – 33 CFR 101.514 states that "federal officials" and "law enforcement officials" are not required to obtain a TWIC to gain unescorted access to secure areas of regulated vessels or facilities. To gain unescorted access, law enforcement officials must identify themselves as such and present their official agency credential for inspection. MTSA /TWIC Policy Advisory Council decision 30-04 (June 17, 2004) and 01-07 (November 21, 2007) provide further guidance on what procedures law enforcement officials should follow to gain access to regulated facilities and vessels and who qualifies under the definition of "law enforcement official." In accordance with their official duties, can law enforcement officials utilize their agency credentials to escort individuals without a TWIC in secure areas of regulated facilities or vessels?

Background – 33 CFR 101.514(b) and (c) state that "federal officials" and "law enforcement officials at the State or local level, are not required to obtain or possess a TWIC to gain unescorted access to secure areas." The definition of "escorting" found in 33 CFR 101.105 states that "Individuals without TWICs may not enter restricted areas without having an individual who holds a TWIC as a side-by-side companion." NVIC 03-07 provides further guidance on how to properly escort non-TWIC holders in secure areas.

Discussion – Though the definition of escorting seems to forbid law enforcement officers from serving as escorts, we consider a law enforcement official's agency- issued credential to be equivalent to TWIC for the purposes of escorting. Federal officials and law enforcement officials are therefore authorized to escort non-TWIC holders within all areas of regulated facilities or vessels in the course of their official duties, particularly when the facility or vessel is one leased or used by a federal agency. Owners and operators will not be penalized for allowing federal and law enforcement officials to escort non-TWIC card holders. Escorting by federal and law enforcement officials shall be accomplished utilizing monitoring or side-by-side physical accompaniment as appropriate for the area where the escorting is to take place utilizing the guidance published in NVIC 03-07.

TWIC/MTSA POLICY ADVISORY COUNCIL

April 1, 2008

Policy
Escorting Standards for 'Persons in addition to Crew'
03-08

Issue – What are the acceptable escorting standards for non-Transportation Worker Identification Credential (TWIC) holding individuals, 'persons in addition to crew,' onboard Offshore Supply Vessels (OSVs), Research, and similar vessels in accommodation spaces?

Background – Title 33, U.S. Code of Federal Regulations (CFR) part 104.265 requires that individuals who do not have a TWIC be escorted, as defined in 33 CFR 101.105, at all times while inside a secure area of the vessel. 33 CFR 101.105 defines "escorting" as "ensuring that the escorted individual is continuously accompanied while in a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted." The definition elaborates that this can be accomplished through side-by-side accompaniment or via monitoring, depending upon where the escorted individual is granted access. In a restricted area, escorting must be side-by-side accompaniment (ratio of 1 TWIC holder to no more than 5 non-TWIC holders, per NVIC 03-07). 33 CFR 104.270 defines security measures and what areas must be designated as restricted areas. In accordance with 33 CFR 104.270(b)(8), crew accommodations are restricted areas.

Discussion – OSVs often transport 'persons in addition to crew' out to mobile offshore drilling units (MODUs) and OCS facilities. Research vessels may have scientists or other non-TWIC holding individuals onboard. Those individuals would need to be escorted or monitored at all times given that the entire vessel is a secure area. Individuals would also need to be escorted through side-by-side accompaniment within all restricted areas on the vessel, including when they are in crew accommodations used to accommodate persons-in-addition-to-crew (i.e. non-TWIC holders) on vessels that do not have separate areas for non-crew members. This presents operational difficulties, as there are not likely to be sufficient vessel personnel holding TWICs onboard to escort the non-TWIC holders in the ratios described in Navigation and Vessel Inspection Circular No. 03-07 published 2 July 2007.

These vessels are required, under 33 CFR 104.285, to have security measures in place for monitoring. These measures should already be included in the vessel's security plan, and ensure the capability to continuously monitor the vessel and restricted areas on board the vessel. The crew (TWIC holders) may monitor a group of "persons in addition to crew" on a vessel underway by observing them and by ensuring that they do not enter unauthorized spaces without an escort. The vessel owner/operator is encouraged to brief non-TWIC holders at the start of the voyage on the location of spaces where they are not authorized, and the owner/operator must ensure that restricted areas are clearly marked.

These measures are sufficient to accomplish the escorting requirement for non-TWIC holders in secure areas that are not also restricted areas.

For the purposes of the maritime security regulations found in 33 CFR Subchapter H, the Coast Guard does not consider all common areas onboard a vessel to be "crew accommodations." For the purposes of 33 CFR subchapter H only, crew accommodations are interpreted as berthing areas used exclusively by crew. Common living areas, such as mess rooms, lounges, recreational spaces, and communal heads shared by crew and persons in addition to crew need not be considered "crew accommodations" for security purposes, and therefore do not need to be restricted areas. Those common areas onboard a vessel that are utilized by both crew members and persons in addition to crew could be designated secure areas through a vessel security plan (VSP) amendment if that designation is supported by the vessel security assessment. Special consideration to the security measures in 33 CFR 104.265 and 33 CFR 104.270 must be given when submitting a VSP amendment. A clear, visual representation (such as a vessel schematic) of the secure and restricted crew accommodation areas should be incorporated into the VSP amendment and kept on board the vessel. Non-TWIC holding individuals could then be monitored in secure areas to satisfy the TWIC requirements in 33 CFR 104.285.

In terms of berthing areas, we envision that vessels that transport 'persons in addition to crew' for extended periods could designate separate berthing for crew members and non-crew members. In that scenario, the berthing areas for crew members would be considered crew accommodations and as such would be considered restricted areas. The berthing areas used exclusively by non-crew members, 'persons in addition to crew,' could be secure, not restricted, areas and the escorting measures described in the second paragraph of this discussion would be sufficient. To accomplish this, a VSP amendment would need to be submitted by the vessel owner/operator to the Coast Guard. The amendment would need to show how and when the vessel would separate berthing areas, as it may vary from voyage to voyage, and specifically include how the restricted areas would be clearly marked from voyage to voyage.

For example, if there are ten staterooms on the vessel, with accommodations for up to six persons in each stateroom, crew could spread out among all staterooms when there are no non-TWIC holding 'persons in addition to crew' on board. In this scenario, all ten staterooms would be restricted areas. If 'persons in addition to crew' were then on board for an extended period, the crew members could temporarily consolidate themselves into one or two staterooms (which would still be restricted areas), and the remaining staterooms, while housing only 'persons in addition to crew' could be secure areas. Magnetic (or other easily moveable) signage could then be used to indicate which staterooms are restricted and which are secure.

If a vessel owner/operator is unable to physically separate berthing areas in a manner similar to the example given above, the vessel must have sufficient personnel holding TWICs on board to provide escorts to the non-TWIC holders in the ratios described in NVIC 03-07, or else the vessel owner/operator must submit (and be granted) a waiver in accordance with 33 CFR 104.130.

TWIC/MTSA POLICY ADVISORY COUNCIL

September 30, 2008

Policy
TWIC Requirements and Rail Access into Secure Areas
05-08

Issue (05-08) – What are the Transportation Worker Identification Credential (TWIC) requirements for railroad workers who, through the normal execution of their duties, require unescorted access to secure areas of Maritime Transportation Security Act (MTSA) regulated facilities? In addition, what is the policy that should be followed by facility owners/operators to address rail line access points?

Background – Title 33, U.S. Code of Federal Regulations (CFR) part 101.514 requires all persons requiring unescorted access to secure areas of facilities regulated by part 105 of subchapter H to possess a TWIC before such access is granted. The term "secure area" is defined as "the area over which the owner/operator has implemented security measures for access control in accordance with their security plan." (See 33 CFR 101.105.) For most facilities, the secure area encompasses the entire facility footprint as described in their currently approved facility security plan (FSP). Due to the integration of various transportation modes for business processes, rail lines may cross into and/or through the secure area of MTSA regulated facilities. Typical freight rail operations at MTSA facilities can present access control and enforcement challenges to facility owners/operators, rail operators, and Coast Guard enforcement personnel. These challenges include: unmanned, non-continuously operated gates at the MTSA facilities, where the rail lines own an easement, have access to keys, locks, or key codes for gates; rail manning realities; and "continuous passage" of the trains, without stopping, through the facility. Both the railroad community and facility owners and operators have requested specific policy guidance pertaining to railroad operations and compliance with the TWIC regulations.

Discussion – 33 CFR 105.255(a)(4) requires owners/operators to prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area. Individuals without a TWIC, at a minimum, are required to show acceptable identification in accordance with 33 CFR 101.515 and be escorted in accordance with procedures required by 33 CFR 105.255(b)(3) and Navigation and Vessel Inspection Circular (NVIC) 03-07.

The feasibility of certain rail workers presenting a TWIC for inspection, as required by 33 CFR 101.514, prior to accessing the facility poses unique challenges. Some rail gates are unmanned and are not continuously operated; the train would most likely need to come to a complete stop prior to entering the facility for TWIC's to be inspected. Escorting railroad crew, in the manner outlined by NVIC 03-07, raises serious safety concerns as only authorized individuals with specialized training should approach, board, transit or work in the vicinity of locomotives,

railcars and railroad tracks. In addition to safety issues, attempting to conduct an escort during railroad operations could detract from the owner/operator and rail crew's ability to observe potential illegal train riders. Carving out the rail line(s) from the facility footprint and/or running fencing along rail lines is likely not feasible.

There are two primary types of railroads that service MTSA facilities: long-haul (Class I) and short line (Class II and Class III). The nature of those types affects the personnel assigned to the individual trains, and therefore the likelihood of their possessing a TWIC. Class II and Class III railroads have fewer employees, a more concentrated or local area of operations, and are most likely already familiar with the security requirements at the facilities they service. Class I railroads are large freight operators which generally cover greater distances, have significantly larger numbers of employees who are often assembled at remote (i.e. not in the general vicinity of maritime ports or TWIC enrollment centers) crewing locations, and interface with multiple facilities and yards across the U.S. Currently, seven Class I and over 500 Class II and Class III freight carriers operate in the U.S. Clearly, the most desirable scenario is for all railroad personnel to possess a TWIC, either while on the train or being brought to the MTSA facility to join a train.

Coast Guard Headquarters personnel have been working with representatives from both types of railroads and MTSA facility representatives on TWIC enrollment issues. In addition, the Coast Guard has taken advantage of one of its advisory committees, the National Maritime Security Advisory Committee (NMSAC), to obtain recommendations concerning TWIC rail policy.

Policy—*Coast Guard National Policy:* It is the Coast Guard's position that, due to the unique aspects of railroad operations that can impact security at MTSA facilities, all railroad crew servicing secure areas of a MTSA facility should possess a TWIC. The Coast Guard recommends railroads view a "MTSA facility crew" as similar to other job qualification prerequisites, such as remote control locomotive operations and territory qualification requirements.

Escorting and Monitoring Railroad Crew: While the regulations allow escort and monitoring accommodation that meets NVIC 03-07 for non-TWIC possessing transportation workers, any accommodation must provide an equivalent level of security, and be captured in the approved FSP. Enforcement, by Captains of the Port, should be directed at ensuring this equivalency. In most cases equivalency may be met as follows:

- In lieu of railroad crew presenting TWIC's for visual examination prior to accessing a MTSA facility in accordance with 33 CFR 101.514, their company's local or regional office/scheduling coordinator could contact the MTSA facility prior to arrival and provide information on the TWIC status of that train's crew. If all crew possess a valid TWIC, no further action would be required by the train operator and MTSA facility operators may permit the train to enter the facility without any further checking of crew TWICs. For trains providing advanced notice that all crew possess a TWIC, only periodic spot checking of TWIC by facility security personnel and COTP personnel is expected. All spot checks should be coordinated with the FSO to ensure adequate safety of personnel.
- If any member of the train crew does not possess a TWIC, the escorting arrangement for those members would need to be approved by the MTSA facility owner/operator, documented as part of the FSP, and approved by the cognizant COTP. This could

include checking to ensure all members of the crew have their identification (as required by 33 CFR 101.515) before the train enters the facility.

- In preparing procedures for acceptable escort and monitoring of the non-TWIC train crew member(s) a front - of - train TWIC holder, back - of - train non-TWIC holder will generally not qualify as an acceptable arrangement for a locomotive moving multiple railroad cars due to the length of the train and the nature of the work associated with operations. Escorting and monitoring procedures must include the ability to quickly notify facility security personnel if an escorted individual is engaged in activities other than those for which the escorted access was granted. It is also recommended that any non-TWIC crew member(s) remain in the immediate vicinity of the train while in secure areas of a MTSA regulated facility. Both the facility and rail crew are expected to monitor for illegal train riders.
- Trains on "continuous passage" through a facility, with proper monitoring, do not have to stop in order to present TWIC's for visual inspection, but the crew would still need to obtain TWICs and the railroad company's local or regional office/scheduling coordinator should also provide an arrival schedule including confirmation that the crew possesses valid TWICs in order to achieve an equivalent level of security. If the train does stop within a secure area of a MTSA regulated facility, the policy discussion in the previous paragraph applies. The facility FSP should describe the means to be used to monitor trains in "continuous passage," which could include closed-circuit video, notification of when the train enters/leaves the facility, or any other method that ensures that the facility security officer, owner, or operator would be able to respond quickly if the train stops.

Responsibilities - *Coast Guard Captains of the Port*: All COTPs should continue outreach to railroads (and their personnel) in their COTP Zone, encouraging enrollment in the TWIC program, and explaining the Coast Guard's positions as outlined above. It is the Coast Guard's policy that significant scrutiny will be applied in evaluating the facility security plan's escort and monitoring provisions for train crews to ensure the security standards for access control in 33 CFR part 105 are being maintained. However, COTPs should allow unique train gate access control provisions in FSPs, provided such an equivalency is demonstrated. Facility monitoring plans for trains on "continuous passage" should also be evaluated prior to FSP approval.

Working with FSO's and railroad safety personnel, COTPs will conduct spot checks of train crews for possession of TWICs while the train and/or crew is within secure areas of the facility. Appropriate enforcement action will follow discovery of a violation of the TWIC provisions of 33 CFR part 105, or the FSP. These violations would be considered a breach of security.

Facility owners/operators: Facility owners/operators should work closely with security personnel from the railroads that service or cross their facility's secure areas. Security measures for access control, as it relates to rail line access points should be stated in procedures to be incorporated into the facility's security plan. In order to provide an equivalent level of security for unmanned gates, facility owners/operators could request railroads servicing their facility to provide the facility with the schedule and the crew's TWIC status. The facility owner/operator should describe in the FSP the plan for periodically validating TWIC possession of train crews and escort/monitoring/response procedures for non-TWIC possessing crewmembers. Trains that pass through facilities, but do not stop for cargo operations (continuous passage), could be handled by allowing the train to pass through the facility without a visual inspection of the

crew's TWICs if the train operator provides the facility with advance notice, the facility or train crew monitors the passage of the train to ensure no one gets on or off, and the train does not stop unexpectedly.

Railroad operators: In addition to communicating directly with MTSA facility owners/operators regarding TWIC, escorting and other access control requirements, railroad operators should enroll personnel in the TWIC program that may be assigned to trains that service or cross MTSA facilities. This will serve to enhance security of the marine transportation system and railroad operations in addition to minimizing potential down time in freight operations as a result of TWIC escort/monitoring/enforcement activities.

TWIC/MTSA POLICY ADVISORY COUNCIL

January 8, 2009

Policy
U.S. Flag Overnight Passenger Vessels in Domestic Trade
"Other Persons in Crew"
01-09

Issue – What are the acceptable escorting standards for non-Transportation Worker Identification Credential (TWIC) holding individuals, 'other persons in crew,' onboard U.S. Flag Overnight Passenger Vessels in Domestic Trade in accommodation spaces?

Background – Title 33, U.S. Code of Federal Regulations (CFR) part 104.265 requires that individuals who do not have a TWIC be escorted, as defined in 33 CFR 101.105, at all times while inside a secure area of the vessel. 33 CFR 101.105 defines "escorting" as "ensuring that the escorted individual is continuously accompanied while in a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted." The definition elaborates that this can be accomplished through side-by-side accompaniment or via monitoring, depending upon where the escorted individual is granted access. In a restricted area, escorting must be side-by-side accompaniment (ratio of 1 TWIC holder to no more than 5 non-TWIC holders, per NVIC 03-07). 33 CFR 104.270 defines security measures and what areas must be designated as restricted areas. In accordance with 33 CFR 104.270(b)(8), crew accommodations are restricted areas.

33 CFR 104.106 allows for ferry, passenger vessels, or cruise ships to designate those areas within the vessel open to passengers as passenger access areas, such as dining rooms, seating areas, parking decks, public restrooms, and bars. 33 CFR 104.107 allows for ferry or passenger vessels, excluding cruise ships, to designate areas within the vessel as employee access areas. Employee access areas are open only to employees, such as galleys, storage areas, dressing rooms, and food service areas. Neither passenger nor employee access areas are secure areas; therefore individuals in passenger or employee access areas would not require a TWIC for unescorted access.

Discussion – U.S. Flag overnight passenger vessels employ persons involved in the support of overnight passengers and ship's crew by providing food, entertainment, and other services such as housekeeping (hereafter referred to as 'other persons in crew'). These employees often conduct the majority of their business in passenger and/or employee access areas. Within these areas, individuals are not required to possess TWICs to gain unescorted access, because they are not part of the vessel's secure area. The rest of the vessel remains a secure area where TWICs are required for unescorted access. Individuals would also need to be escorted through side-by-side accompaniment within all restricted areas on the vessel, including when they are in crew accommodations. This presents operational difficulties, as there are not likely to be

sufficient vessel personnel holding TWICs onboard to escort the non-TWIC holders in the ratios described in Navigation and Vessel Inspection Circular No. 03-07 published 2 July 2007.

In terms of berthing areas, we envision that passenger vessels that employ 'other persons in crew' could designate separate berthing for crew members and other persons in crew. In that scenario, the berthing areas for crew members would be considered crew accommodations and as such would be considered restricted areas. The berthing areas used exclusively by other persons in crew could be designated employee access areas and as such TWICs would not be required for unescorted access. To accomplish this, a VSP amendment would not need to be submitted. However, if berthing for other persons in crew is designated an employee access area, the owner/operator must maintain a visual representation (e.g. a vessel schematic) onboard the vessel with the approved VSP detailing where these areas are located as required by 33 CFR 104.120(c). Vessels operating under an ASP must also maintain this visual representation onboard if they designate these areas. This visual representation does not need to be approved by the Coast Guard until the next VSP submission, but must be available during Coast Guard inspections. VSPs must be updated to include the visual representation with the next submission, either amendment or renewal. In addition, for access control security measures, the restricted areas would be clearly marked as required by 33 CFR 104.270.

If a vessel owner/operator is unable to physically separate berthing areas in order to designate some of them as employee access areas, the vessel must have sufficient personnel holding TWICs on board to provide escorts to the non-TWIC holders, as described in NVIC 03-07, or else the vessel owner/operator must submit (and be granted) a waiver in accordance with 33 CFR 104.130.

TWIC/MTSA POLICY ADVISORY COUNCIL

January 22, 2009

Policy
Training Requirements for Escorts on Regulated Facilities and Vessels
02-09

Issue – What are the training requirements for TWIC holders who act as escorts for non-TWIC holders, but do not perform security duties as a primary function of their job, including third party escort providers?

Background – Individuals seeking to gain entry to a vessel, facility, and OCS facility regulated by parts 104, 105, or 106 of 33 CFR Subchapter H must be under escort while inside a secure area by an individual who possesses a valid TWIC if they do not possess a valid TWIC. Escorting, defined in 33 CFR 101.105, means ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted. This may be accomplished utilizing monitoring or side-by-side physical accompaniment as appropriate for the area where the escorting is to take place (secure, non-restricted or secure, restricted), utilizing the guidance published in NVIC 03-07.

The owner/operator is responsible for determining how escorting will be carried out in accordance with the regulations found in 33 CFR Subchapter H and further guidance found in NVIC 03-07.

Discussion – Individuals that monitor or provide side-by-side physical accompaniment must possess a valid TWIC. Escorts are not always considered "facility personnel with security duties" because they do not perform security duties as a primary function of their employment. Additionally, some facility or vessel owner/operators may authorize non-direct employees to conduct escorting duties aboard their facility or vessel. For TWIC holders to escort non-TWIC holders on MTSA regulated vessels, facilities, and OCS facilities; they shall meet the training requirements listed in 33 CFR 104.225, 105.215, or 106.220, respectively. Specifically, escorts must have knowledge of owner/operator's escorting procedures, and the procedures and contingency plans determined by the owner/operator if an escorted individual is engaged in activities other than those for which escorted access was granted.

TWIC/MTSA Policy Advisory Council decision 02-08 (January 25, 2008) provides further guidance outlining the requirements for federal and law enforcement officials to escort non-TWIC holders within secure areas. Federal and law enforcement officials will not be required to receive training in accordance with 33 CFR 104.225, 105.215, or 106.220.

TWIC/MTSA POLICY ADVISORY COUNCIL

June 9, 2009

Policy
Escorting Requirements for Passengers Traveling
With Commercial Truck Drivers
06-09

Issue – Are passengers riding with commercial truck drivers required to obtain a Transportation Worker Identification Credential (TWIC) if they stay within the cab of the vehicle while in secure areas of a facility regulated by the Maritime Transportation Security Act (MTSA)?

Background – The TWIC Program aims to enhance security by ensuring that individual's granted unescorted access to secure areas of MTSA regulated facilities have passed a security threat assessment (STA) and received a tamper resistant biometric enabled credential. During the enrollment process, as outlined in Title 49 U.S. Code of Federal Regulations (CFR) part 1572.17, applicants are required to certify in writing that they must obtain a TWIC as part of their employment duties, are required to have unescorted access to secure areas of facility or vessel regulated by the Maritime Transportation Security Act (MTSA) per 33 CFR 104, 105, or 106, respectively, are a U.S. Coast Guard credentialed merchant mariner (or applying to be a U.S. Coast Guard credentialed merchant mariner), and/or are a commercial driver licensed in Canada or Mexico transporting hazardous materials in accordance with 49 CFR 1572.201. Title 49 CFR 1570.5 holds an individual liable if they make any fraudulent or intentionally false statement throughout the TWIC enrollment process.

Discussion – In Navigation and Inspection Circular (NVIC) 03-07, the Coast Guard outlined the expectation that "individuals who frequently access secure areas in the course of their employment will obtain TWICs and therefore will be eligible for unescorted access." Due to the unique nature of commercial truck drivers, they may choose to travel with a passenger throughout the course of their work assignments. In many cases, the passenger does not require frequent access to MTSA facilities, meet the eligibility requirements to obtain a TWIC, and/or have access to adequate infrastructure to remain safely outside of the secure area while waiting for the trucker to complete their work obligations.

Facility owners/operators may set their own policies on who may act as an escort, including establishing specific training requirements for doing so in accordance with 33 CFR 105.215. This may present a hardship for truck drivers who travel with passengers in the cab of their vehicle because some facility owner/operators may refuse to allow the truck driver, who holds a TWIC, to act as an escort for their passengers and the truck driver may have difficulty in meeting training requirements set by individual facilities.

Policy - The Coast Guard has determined that, at the discretion of the facility security officer, it is acceptable for a facility to allow a truck driver holding a TWIC to escort passengers without a

TWIC on facilities regulated by 33 CFR part 105, so long as they meet all of the following criteria:

- the passenger does not require a TWIC in their own right, per 33 CFR 101.514;
- the passenger remains within the cab of the vehicle for the duration of the time that the vehicle remains within a secure area;
- the facility owner/operator agrees to permit the trucker to escort his/her passenger;
- the passenger can present personal identification that meets the requirements of 33 CFR 101.515, unless age prevents issuance of a qualifying ID;
- there is no suspicious behavior or actions on the part of the passenger or truck driver requesting to perform escorting duties;
- the passenger's age or presence within the secure area will not interfere with facility safety policies/procedures;
- the commercial truck driver possesses a valid TWIC and meets the minimum training requirements listed in 33 CFR 105.215 (Security training for all other vessel/facility/OCS facility personnel) and any additional training requirements established by the facility; and
- the commercial truck driver must have knowledge of the owner/operator's escorting procedures, and the procedures and contingency plans determined by the owner/operator if an escorted individual is engaged in activities other than those for which escorted access was granted. (The owner/operator is responsible for providing this information to the truck driver by classroom-style, one-to-one briefings, or via fliers/handouts outlining the various information that the escort needs to know. For further guidance, refer to Policy Advisory Council (PAC) Decision 02-09 dated 22 JAN 09.)

Since TWIC is a component of the MTSA, facility owners/operators must continue to inspect the personal identification, per 33 CFR 101.515, for passengers of commercial truck drivers. Examples of personal identification may include: a driver's license, state issued ID, passport, or other government issued personal ID. Although the Coast Guard sees this as an acceptable access control procedure, the facility owners/operators are required to implement access control procedures and have the right to require a TWIC from the passengers despite the unique circumstances.

Coast Guard guidance does not supersede existing federal, state, or local regulations regarding who may or may not be granted access to facilities. The facility owner/operator is responsible for following any existing safety and/or security requirements with which the facility is legally required to comply. At the owner/operators discretion, this PAC decision may be used as an option to allow truck drivers holding a valid TWIC, to escort passengers without a TWIC on facilities regulated by 33 CFR 105.

TWIC/MTSA POLICY ADVISORY COUNCIL

July 15, 2009
Updated August 31, 2009

Policy
Incorporating TWIC into Existing Physical Access Control Systems

08-09 Change 1 * CG-FAC Edited 2018

Background – On July 2, 2007, the Coast Guard published Navigation and Vessel Inspection Circular (NVIC) 03-07, Guidance for the Implementation of the Transportation Work Identification Credential (TWIC) Program in the Maritime Sector. The purpose of this NVIC was to prepare and assist field units and industry partners for compliance with the TWIC final rule which was published on January 25, 2007.

Incorporation of the TWIC into Existing Physical Access Control Systems was addressed in NVIC 03-07. However, in response to recent feedback from field units and industry regarding the potential for misinterpretation of this section, this Policy Advisory Council (PAC) decision provides additional clarification and policy pertaining to this issue.

Discussion – Incorporating TWIC into existing physical access control systems – The intent of NVIC 03-07 was to allow vessels or facilities with existing electronic physical access control systems to continue to utilize their company-issued local access cards for entry while final regulations for TWIC card readers were developed. The NVIC authorized use of existing electronic physical access control systems, as long as the system could support a match between the local access card and the individual's valid TWIC upon each entry. The desired benefit to owners/operators was the ability to continue to use a system that was already in place, prior to full TWIC implementation utilizing credential readers, which interfaced with a local access badge.

Title 33 Code of Federal Regulations (CFR) parts 104.265(c)(1) and 105.255(c)(1) require the owner or operator to implement TWIC into their access control measures and ensure that persons seeking unescorted access to secure areas of their vessel or facility present their TWIC for inspection prior to authorizing entry. The owner/operator's TWIC inspection must include: a match of the photo in the TWIC to the individual; verification that the TWIC has not expired; and a verification of the various security features of the credential. Vessel and facility owner/operators who elect to utilize the provisions of NVIC 03-07 are considered to be meeting only the card authentication and card validity requirements found in 33 CFR part 104.265(c)(1)(ii) & (iii) or 105.255(c)(1)(ii) & (iii), as appropriate.

The example provided in NVIC 03-07 states the "TWIC does not need to be used as a visual identity badge for each entry." This is still USCG policy; however, identity verification of the individual utilizing a company credential or access card is still required before unescorted access may be granted to secure areas, as stated in NVIC 03-07, and in accordance with 33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i), as appropriate. Verification is necessary to ensure the company card is not being utilized by another individual who may be unauthorized. This verification could be accomplished via gate guard, Closed Circuit Television (CCTV) or other means acceptable to the relevant Coast Guard Captain of the Port (COTP).

The aim of the Coast Guard remains the same. The Coast Guard seeks to enhance the security of ports and vessels by ensuring that only persons who hold valid TWICs are granted unescorted access to secure areas of MTSA regulated vessels and facilities.

Policy – Coast Guard policy found in NVIC 03-07 is as follows:

1. Owners/operators must be capable of demonstrating to Coast Guard inspectors that issuance of a unique local access card to an individual, allowing the individual unescorted access into the secure area of the vessel or facility, is tied to verification of a valid TWIC being issued to the individual. Initial verification of the TWIC must meet all of the inspection requirements in 33 CFR 104.265(c)(1) or 105.255(c)(1) (as appropriate). An individual who does not hold a valid TWIC must not hold a company-issued local access card that allows unescorted access into secure areas.
2. Once a TWIC is verified to be valid, and until the Coast Guard publishes a final rule requiring the use of TWIC readers as an access control measure, a company issued local access card can be used for unescorted access to secure areas. Identity verification (33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i)), must still be performed to ensure the individual presenting the company issued local access card is the individual authorized unescorted access. This means that a match of the photo on the company card to the individual must occur.
3. Continued use, by an individual, of the company-issued local access card to gain access to secure areas of the vessel or facility is authorized based on the vessel's or facility's verification that the individual's TWIC remains valid in accordance with 3.3.f of NVIC 03-07 prior to authorizing unescorted access to a secure area.
4. Unescorted individuals, who have gained access within a vessel's or facility's secure area using the company-issued local access card, must still be in possession of their TWIC, or be able to retrieve it within a reasonable time, as required by 33 CFR 101.515(d)(1) & (2). If during the check of the TWIC it is found to be invalid, the company-issued local access card to the secure area is also invalid. Appropriate action by the Coast Guard will follow if a person is found to not be in possession of a valid TWIC.
5. Use of existing electronic card readers designed to work with TWICs, is authorized to meet the requirements for card authentication and card validity (33 CFR 104.265(c)(1)(ii) & (iii) or 105.255(c)(1)(ii) & (iii)). Identity verification (33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i)), in which a match of the photo on the TWIC is compared with the individual presenting the TWIC, must still be performed separately. Identity verification can be accomplished by utilizing a

gate guard to match the photo to the individual, use of CCTV to perform the match, or other means acceptable to the COTP. Matching the biometric template stored on the TWIC to the TWIC holder's fingerprint as the sole process to verify identity is not authorized at this time. Government testing and evaluation of currently available readers is on-going and additional regulatory requirements and policy guidance will be needed prior to full utilization of reader capabilities to meet all inspection requirements.

NOTE:

(1) For any **facility that does not meet the provisions of the identity verification in this PAC,** due to previously installed access control systems and/or infrastructure, the following procedures shall be utilized in order to mitigate any potential security risks:
   a. At MARSEC Level 1 –Random checks for TWIC must be conducted of individuals accessing secure areas at the rate specified on the secure (password-protected) side of HOMEPORT at http://homeport.uscg.mil (all inspection requirements under 33 CFR 105.255(c)(1) must be conducted, including the identity verification component).
   b. At MARSEC Level 2 & 3 –Verification at the rate specified on the secure (password-protected) side of HOMEPORT to include identity verification, card validity, and card authentication must be conducted via a company issued badge or TWIC prior to being granted unescorted access to secure areas.
   c. The random TWIC inspection requirements discussed above are in addition to the performance standards for screening found in MARSEC Directives 105-1, 2, & 3.

(2) Any facility utilizing the above provisions must submit an FSP amendment to the cognizant COTP in accordance with 33 CFR 105.415(a) detailing the implementation of these alternate access control procedures.

(3) The above guidance is intended for use during the transition period leading up to the promulgation of a TWIC reader final rule, at which time it is anticipated that use of legacy access control systems that are not compatible with a TWIC will no longer be acceptable for use. Any access control system or infrastructure must be in full compliance with the requirements of 33 CFR 105.255(c)(1).

MTSA POLICY ADVISORY COUNCIL

July 29, 2009

Policy

Waiving Facilities that Transfer and Store Asphalt
09-09 Change 1

*CG-FAC Edited 2018

FINAL

Issue: Asphalt (aka Asphalt Cement, Neat Asphalt) describes a variety of low combustibility, low flammability, liquid hydrocarbons that are regulated under 33 CFR 154. Because of applicability to these safety and pollution prevention regulations, asphalt facilities are also placed into the MSTA regulatory regime contained in 33 CFR Subchapter H. However, given the physical properties of asphalt, should facilities that transfer and store asphalt be waived from the requirements of 33 CFR part 105?

Discussion: 33 CFR 105.105(a)(1) requires facilities that are regulated under 33 CFR part 154 to also be regulated under 33 CFR part 105. This was done for the entire category of oil products because of the potential that, if attacked or used as a weapon, the physical properties of many of these cargoes would likely result in a transportation security incident (TSI).

Asphalt generally has a flash point of >450^{o}F, and an ignition temperature of >700^{o}F. It has an OSHA flammability classification of Class IIIB, with a flash point at or above 200^{o}F and, therefore, OSHA flammable and combustible liquid regulations do not apply. This also means that, for practical purposes, someone initiating a security incident by attacking a cargo or storage tank of asphalt would first need to heat the cargo significantly to produce a fire. Moreover, facilities that handle asphalt cargoes typically store the asphalt in very large above ground storage tanks often with a capacity of 500,000 gallons or more. This makes it extremely difficult for a terrorist to heat up such a large tank of asphalt to a temperature to cause it to burn or to get it to detonate. This makes an intentional attack on an asphalt tank implausible and unlikely to result in a TSI due to significant loss of life.

Asphalt is stored at elevated temperatures (300^{o}F) to allow the product to be moved through pipelines and hoses as a liquid. It is stored at facilities in above ground tanks surrounded by an EPA approved spill containment berms. Areas enclosed by these berms are, by EPA regulation, sufficient in size to hold the entire contents the storage tank. This keeps the contents of a leaking tank within the boundary of the berm and greatly aids in recovery of the product and mitigation of harm to the environment. It is possible that an attack on a large above ground asphalt tank could result in a near instantaneous release of the tank's content and resulting wave of flowing asphalt that would flow over

the spill prevention berm. However, once released, the asphalt would begin to cool and harden. These characteristics make asphalt releases on the land relatively easy to mitigate and not likely to result in significant environmental damage.

In September, 2008, DOT Pipeline and hazardous Materials Safety Administration issued a proposed rule entitled, *Hazardous Materials: Risk Based Adjustment of Transportation Security Plan Requirements*. Concluding that the likelihood of terrorist action against asphalt carriers (Class 9) was remote therefore the security risk associated with the transportation of these materials was not sufficient to warrant development of security plans.

Decision: Asphalt transfer and storage are low risk operations. If asphalt storage tanks were to be attacked it is unlikely there would be significant loss of life, damage to the environment, significant disruption to the transportation system or to the area's economy.

Facilities wishing to have their operations examined in consideration for a waiver may forward a request to Commandant (CG-FAC-2) in accordance with 33 CFR 105.130. No waiver request will be approved if the cognizant COTP feels that security would be compromised in his/her AOR. The request letter should address the following areas:

1. Does the facility store more than 42,000 gallons of any other 33 CFR 154 regulated cargo?
2. Does the facility receive any vessels subject to SOLAS?
3. Does the facility receive foreign flagged vessels?
4. Does the facility receive passenger vessels?
5. Is the facility regulated under any other applicability factor.

Questions can be directed to:

UNITED STATES COAST GUARD
COMMANDANT (CG-FAC-2) STOP 7501
OFFICE OF PORT & FACILITY COMPLIANCE
2703 MARTIN LUTHER KING JR AVE SE
WASHINGTON, DC 20593-7501

MTSA POLICY ADVISORY COUNCIL (PAC)

September 9, 2009

Policy

Defining what areas of a Barge Fleeting Facility are subject to Subchapter H part 105 security requirements

10-09

FINAL

Issue: When the MTSA regulations were published and Facility Security Plans (FSPs) for Barge Fleet Facilities (BFFs) were written, the regulations were not uniformly applied by the Coast Guard or fleet facilities to property owned or operated by barge fleeting companies. The result was the inconsistent application and enforcement of MTSA regulations at similarly configured and/or operated BFFs. For example, some BFFs included large portions of adjacent shore-side property owned and operated by the company while others included little to none. The inclusion of shore-side property not having any applicability under 33 CFR 105.105 could result in property such as wash and towboat docks, office space and topside repair yards that would not normally be subject to MTSA regulations being identified as a secure area.

References: 33 CFR 105.255 & 105.296; NVIC 03-07 (3.4)

Discussion: The maritime transportation portion of a BFF at risk of being involved in a transportation security incident (TSI) (as defined in 33 CFR 105.105(a)(6)) is normally limited to the area where the regulated barges are fleeted and/or moored. A BFF is often separated from the related shore-side area by water, tree lines, and/or swamps, which constitute natural barriers to the shore-side area. In many cases, barge fleets are only accessible by vessel. Normally, land in the immediate vicinity of a BFF (whether or not controlled or operated by the barge fleet) and not involved in the transfer or storage of regulated cargo is not considered to be at risk of a TSI.

Policy: BFFs can limit their MTSA footprint to the free-floating barge tiers that fleet MTSA regulated barges. This footprint should be defined in the FSP (e.g. left descending bank Mississippi River MM 146.8 to MM 146.6 and MM 146.3 to MM 146). BFF Security Plans (FSP) will include security measures taken at all access points leading to secure and/or restricted areas. This may include accessibility to the regulated barge tiers directly from shore (i.e., no natural barrier as described in the discussion), vessels providing transportation to restricted barge tiers, and access to restricted areas that are outside of secure areas (see NVIC 03-07 (3.4 a)(3)). For example, some shore-side areas, such as a fleet boat dock, serve as embarkation points for persons needing access to a BFF. In this case, the FSP should include and/or detail access control measures provided by the facility and the vessel that ensure security of the fleet from unauthorized persons who may be transiting from non-secure areas. For the purpose of TWIC applicability, the fleet boats, crew boats, and all personnel allowed on tiered barges will be TWIC holders approved for entry by the BFF FSO or be escorted by TWIC-holder company personnel. Additionally, the FSP should include procedures for controlling Sensitive Security Information (SSI) such as the FSP and other records required by 33 CFR 105.225 following the guidance provided in 49 CFR parts 15 and 1520.

This PAC decision is consistent with 33 CFR 105.296(a)(4), which states that the regulated entity should control access to the barges once tied to the fleeting area by implementing TWIC as described in 33 CFR 105.255.

TWIC/MTSA POLICY ADVISORY COUNCIL

MARCH 15, 2011

Policy
Voluntary Use of TWIC Readers

01-11

Issue – In accordance with the Maritime Transportation Security Act (MTSA) and Security and Accountability for Every (SAFE) Port Act, it is clear that Congress intended the use of transportation security card readers to leverage the full security benefits of Transportation Worker Identification Credential (TWIC). The Department of Homeland Security (DHS), the U.S. Coast Guard, and the Transportation Security Administration (TSA) are still developing TWIC reader requirements as the reader pilot progresses. As such, many facility owner/operators who received grant funding have been reluctant to move forward on purchasing TWIC equipment.

Background – A TWIC Notice of Proposed Rulemaking (NPRM), which included both credential and credential reader requirements, was published on May 22, 2006. Based on public and stakeholder input, DHS decided to split the final rulemaking and removed the reader requirements to be considered in a future rulemaking once contactless reader capabilities for TWIC could be established. That future rulemaking will cover a much broader range of issues related to TWIC readers than does this policy, including but not limited to specific card authentication, validation and identity verification requirements. The TWIC Final Rule implementing the credential requirements published on January 25, 2007.

On July 2, 2007, the Coast Guard published Navigation and Vessel Inspection Circular (NVIC) 03-07, Guidance for the Implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector. The purpose of this guidance document was to prepare and assist field units and industry partners for compliance with the TWIC Final Rule. It included a discussion on how to incorporate the TWIC requirements from the Final Rule into existing physical access control systems (NVIC 03-07).

After encountering requests for clarification on this guidance, the Coast Guard published Policy Advisory Council (PAC) Decision 08-09, Incorporating TWIC into Existing Physical Access Control Systems - Change 1 on August 31, 2009. PAC Decision 08-09 Change 1 provided guidance explaining that the Coast Guard viewed as TWIC compliant vessels or facilities with existing electronic physical access control systems that continue to use company-issued local access cards for entry, as long as the system supports a match between the local access card and the individual's valid TWIC upon each entry. At that time, use of existing electronic card readers, designed to work with the TWIC, was authorized to meet the requirements for card authentication and card validity (33 CFR 104.265(c)(1)(ii) & (iii), 105.255(c)(1)(ii) & (iii), or 106.260(c)(1)(ii) & (iii)).

Identity verification, in which a match of the photo on the TWIC is compared with the individual presenting the TWIC, had to be performed separately (33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i) or 106.260(c)(1)(i)). Matching the biometric template stored on the TWIC to the TWIC holder's fingerprint as the sole process to verify identity was not authorized at that time.

The SAFE Port Act requires DHS to conduct a card reader pilot program to test the business processes and technology required to deploy transportation security card readers as well as examine operational impacts for vessel and facility owners and operators. It also requires a report to Congress that provides the results of the pilot. The statute further requires any final TWIC reader rule be consistent with the findings of the pilot program. DHS will issue an NPRM incorporating the data and conclusions into the proposal and its supporting analyses. This will satisfy the SAFE Port Act requirement, and ensure the public has time to comment on the proposed rule before DHS publishes a final rule. (Initial government testing and evaluation of available TWIC readers has been completed; but additional testing of new readers is an ongoing process. Additionally, there are owners/operators who have been awarded DHS Port Security Grants for the purpose of purchasing and installing TWIC readers and systems, whose funding will expire if it is not expended before 2012).

For these reasons, the Coast Guard has re-examined the capability for TWIC readers to verify identity, using biometric match, in a manner that may be deemed equivalent to the visual card inspection requirements in 33 CFR 104.265(c)(1)(i), 105.255(c)(1)(i), and 106.260(c)(i).

Policy – All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with 33 CFR 101.514. At each entry, the TWIC must be checked for: (1) identity verification, (2) card validity, and (3) card authentication.

(1) Identity verification ensures that the individual presenting the TWIC is the same person to whom the TWIC was issued. The current requirement for identify verification is to compare the photo on the TWIC to the person at the access point (33 CFR 104.265(c)(1)(i), 105.255(c)(1)(i)), or 106.260(c)(1)(i)).

In accordance with 33 CFR 101.130, the Coast Guard determines that a biometric match using a TWIC reader from the TSA list of readers that have passed the Initial Capability Evaluation (ICE) Test (available at: http://www.tsa.gov/assets/pdf/twic_ice_list.pdf) to confirm that the biometric template stored on the TWIC matches the fingerprint of the individual presenting the TWIC meets or exceeds the effectiveness of the identity verification check.[1]

(2) Card validity involves the determination that a TWIC has not expired; been reported lost, stolen, or damaged; or been revoked for cause by TSA. The current requirement for

[1] Any TWIC reader authorized by this guidance to meet the identity verification requirement at 33 CFR 104.265(c)(1)(i), 105.255(c)(1)(i)), or 106.260(c)(1)(i) may no longer be valid after the promulgation of a TWIC reader final rule requiring the use of readers during access control procedures.

card validity is visual inspection to check that the TWIC has not expired (33 CFR 104.265(c)(1)(ii), 105.255(c)(1)(ii), or 106.260(c)(1)(ii)).

In accordance with 33 CFR 101.130, the Coast Guard determines that using a TWIC reader to check for card validity by either[2]:

(a) comparing the card's internal Federal Agency Smart Card Number (FASC–N) to the TSA Cancelled Card List or
(b) using a Certificate Revocation List (CRL) meets or exceeds the effectiveness of the card validity check.

(3) Card authentication ensures that the card being used is an authentic TWIC. The current requirement for card authentication is visual and/or physical inspection of various security features present on the card (33 CFR 104.265(c)(1)(iii), 105.255(c)(1)(iii), or 106.260(c)(1)(iii)).

In accordance with 33 CFR 101.130, the Coast Guard determines that card authentication with a TWIC reader to perform the CHALLENGE/RESPONSE protocol using the Card Authentication Certificate and the card authentication private key on the TWIC meets or exceeds the effectiveness of the card authentication.[3]

(4) Owners/operators using biometric readers that are on the TSA list of readers that have passed the Initial Capability Evaluation (ICE) Test should ensure that the readers are operated and maintained according to manufacturer's instructions; and operated by individuals who are trained in the use of said readers.

(5) Any vessel or facility owner/operator using the above provisions must submit a Vessel Security Plan or Facility Security Plan amendment to the Marine Safety Center, cognizant Captain of the Port, or District Commander in accordance with 33 CFR 104.415(a), 105.415(a), or 106.415(a). The amendment must detail the implementation of a TWIC reader system as an equivalent access control procedure to the one established by 33 CFR 104.265(c)(1), 105.255(c)(1), or 106.260(c)(1), as applicable.

(6) PAC Decision 08-09, Incorporating TWIC into Existing Physical Access Control Systems - Change 1, remains valid for vessels or facilities with existing electronic physical access control systems as long as the systems can support a match between the local access card and the individual's valid TWIC upon each entry. PAC Decision 08-09 allows owners and operators to use existing (non-TWIC) electronic cards, readers, and physical access control systems to meet the requirements for card authentication and validity ONLY. Visual inspections of the TWICs at the prescribed rate would still be required.

[2] Any TWIC reader authorized by this guidance to meet the card validity requirement at 33 CFR 104.265(c)(1)(ii), 105.255(c)(1)(ii), or 106.260(c)(1)(ii) may no longer be valid after promulgation of a TWIC reader final rule on access control procedures.
[3] Any TWIC reader authorized by this guidance to meet the card authentication requirement at 33 CFR 104.265(c)(1)(iii), 105.255(c)(1)(iii), or 106.260(c)(1)(iii) may no longer be valid after promulgation of a TWIC reader final rule on access control procedures.

Note: TWIC readers allowed pursuant to this interim guidance may no longer be valid after promulgation of a TWIC reader final rule requiring the use of readers during access control procedures. DHS will not fund replacement readers. Any grandfathering or phase-in period considerations will be addressed in the rulemaking process, providing adequate opportunity for comment, but should in no way be inferred from this interim guidance.

Return to Contents

-End-